UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

TRABAJO FIN DE GRADO

IMPLEMENTACIÓN DEL PROCEDIMIENTO "LOCATION UPDATE" DE GSM EN PLATAFORMA SOFTWARE DEFINED RADIO

DEPARTAMENTO DE TEORÍA DE LA SEÑAL Y COMUNICACIONES

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

AUTOR: FERNANDO RABADÁN QUESADA

TUTOR: DR. VÍCTOR P. GIL JIMÉNEZ

Leganés, Septiembre de 2015

Agradecimientos

En primer lugar me gustaría agradecer a mi tutor, el Dr. Víctor P. Gil Jiménez, por haberme dado la oportunidad de realizar este trabajo, guiándome en el desarrollo del mismo y atendiendo las dudas que me surgían.

A mis amigos, por estar siempre disponibles cuando necesitaba desconectar y pasar un rato al margen del proyecto.

También quiero agradecer a todos los profesores que he tenido durante este tiempo, sin ellos no habría podido llegar hasta aquí.

No puedo olvidarme de mis compañeros de clase, con los que he compartido los últimos cuatro años llenos de grandes momentos.

Por último, quiero agradecerle a mi familia todo el apoyo que me ha dado siempre, animándome y confiando en mí durante este importante periodo.

Resumen

Este TFG consiste en la implementación de uno de los procedimientos más comunes dentro de las comunicaciones móviles en una plataforma SDR (S*oftware-Defined Radio*). Este procedimiento es el "Location Update" de GSM, que se produce cuando un móvil cambia de estación base. Para el desarrollo del mismo se han usado los transceptores de National Instruments USRP-2920 y el software LabVIEW.

El desarrollo del trabajo se centra en la interfaz radio de GSM, realizando todos los procesos que se llevan a cabo tanto en el móvil como en la estación base para intercambiar los mensajes usados en el procedimiento. De esta forma, se logra simular una comunicación lo más fiel posible a la real, con todos los pasos que sigue un mensaje en GSM desde que se genera en un terminal, hasta que llega a otro y este lo trata y consigue el mismo mensaje original.

Palabras clave: SDR, LabVIEW, USRP, GSM, mensaje, slot, ráfaga, trama.

Abstract

This TFG consists in implementing one of the most common procedures in mobile communications in a SDR (S*oftware-Defined Radio*) platform. This procedure is the GSM "Location Update", which takes place when a mobile phone changes his base station. The SDR platform used to develop this work is composed of the National Instruments USRP-2920 transceivers and LabVIEW software

The development of this project focuses on the GSM radio interface, conducting all the processes that are performed in both, mobile station and base station, so as to exchange the messages used in the procedure. This way, we create a simulation as faithful as possible to reality, with all the steps that follows a GSM message from when it is generated in one terminal, till it reaches another and this one treats it and obtains the same original message.

Keywords: SDR, LabVIEW, USRP, GSM, message, slot, burst, frame.

Contenido

Índice de figuras

Índice de tablas

Glosario

AGCH	*Access Grant Channel*
AuC	*Authentication Centre*
BCC	*Base Station Color Code*
BCH	*Broadcast Control Channel*
BCCH	*Broadcast Common Control Channel*
BSC	*Base Station Controller*
BSIC	*Base Station Identity Code*
BSS	*Base Station Subsystem*
BTS	*Base Transceiver Station*
CBCH	*Cell Broadcast Channel*
CCCH	*Common Control Channel*
CCH	*Control Channel*
CEPT	*Conférence européenne des administrations des postes et des télécommunications*
CM	*Call Management*
EIR	*Equipment Identity Register*
FACCH	*Fast Associated Control Channel*
FCCH	*Frequency Correction Channel*
FDD	*Frequency Division Duplexing*
FDMA	*Frequency Division Multiple Access*
GMSC	*Gateway Mobile services Switching Centre*)
GMSK	*Gaussian Minimum Shift Keying*
GSM	*Global System for Mobile Communications*

HLR	*Home Location Register*
HSPA	*High-Speed Packet Access*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
LabVIEW	*Laboratory Virtual Instrumentation Engineering Workbench*
LAC	*Location Area Code*
LAI	*Location Area Identification*
LPI	*Ley de Propiedad Intelectual*
LTE	*Long Term Evolution*
MCC	*Mobile Country Code*
MM	*Mobility Management*
MNC	*Mobile Network Code*
MS	*Mobile Station*
MSISDN	*Mobile Station Integrated Services Digital Network*
MSC	*Gateway Mobile services Switching Centre*)
MSK	*Minimum Shift Keying*
MSRN	*Mobile Subscriber Roaming Number*
NI	*National Instruments*
NSS	*Network and Switching Subsystem*
OSS	*Operation Support Subsystem*
PCH	*Paging Channel*
PSTN	*Public Switched Telephone Network*
RACH	*Random Access Channel*
RPE-LPT	*Regular Pulse Excited – Long Term Prediction*

RR	*Radio Resources Management*
SACCH	*Slow Associated Control Channel*
SCH	*Synchronization Channel*
SDCCH	*Stand Alone Dedicated Control Channel*
SDF	*Software-Defined Radio*
SIM	*Subscriber Identity Module*
TCH	*Traffic Channel*
TDMA	*Time Division Multiple Access*
TFG	*Trabajo Fin de grado*
TMSI	*Temporary Mobile Subscriber Identity*
TN	*Timeslot Number*
TSC	*Training Sequence Code*
UMTS	*Universal Mobile Telecommunications System*
USRP	*Universal Software Radio Peripheral*
VI	*Virtual Instrument*
VLR	*Visitor Location Register*

1. Introducción

1.1. Versión en español

1.1.1. Motivación

Desde su origen, los sistemas de telecomunicación han funcionado haciendo uso de un hardware específico para cada función que realizan. Sin embargo, hace dos décadas ya surgió el concepto de SDR (*Software-Defined Radio*), que hace referencia a un sistema de radiocomunicaciones en el que los componentes hardware específicos están implementados mediante software a través de un procesador de carácter más general.

Con el fin de explotar las posibilidades de estas plataformas SDR, el departamento de Teoría de la Señal y Comunicaciones de la Universidad Carlos III de Madrid ha ido proponiendo trabajos basados en esta tecnología. Más concretamente, este trabajo surge como complemento del TFG de Isaac Morcillo [1], en el que se implementaba un receptor simple de GSM [2] en esta plataforma SDR.

Con la realización de este trabajo se pretende conseguir desarrollar una parte del funcionamiento de GSM. Esta parte, junto con los proyectos que otros compañeros realizaron anteriormente y los que se hagan en el futuro, puede servir como ejemplo del potencial de estas plataformas SDR, ya que se puede lograr simular de forma prácticamente completa el estándar de GSM.

1.1.2. Objetivos

El principal objetivo de este trabajo es conseguir implementar en una plataforma SDR todo el proceso que se lleva a cabo cuando un móvil que está en una red GSM cambia de zona y pasa a estar bajo la cobertura de una nueva estación base (BTS). Este proceso, que recibe el nombre de "Location Update", consiste en el envío y recepción de una serie de mensajes definidos.

Por lo tanto, lo que se pretende es crear esos mensajes desde cero y que sigan el proceso que se realiza en la realidad. Dicho proceso incluye la codificación del mensaje según el canal lógico que le corresponde, la organización de estos mensajes en tramas para ser enviados, la modulación GMSK que se usa en el estándar y, por la parte del receptor, todo el proceso inverso para obtener el mensaje original.

Como el principal cometido de este trabajo es ilustrar el procedimiento concreto, no se ha implementado de forma estricta todo el proceso de sincronización que sí se tiene en GSM, es por ello que el envío y recepción de mensajes se hará de una forma más directa y sin una sincronización rigurosa.

Por último, la finalidad principal de este trabajo no es otra que servir de ejemplo para estudiantes de asignaturas relacionadas con las comunicaciones móviles, de forma que en un futuro puedan realizar alguna práctica de laboratorio o trabajo en el que se use el programa desarrollado.

1.1.3. Estructura de la memoria

Para facilitar la tarea al lector y que la lectura resulte coherente, la memoria se divide en siete capítulos:

- **Capítulo 1: Introducción** – Se expone la motivación del trabajo y su finalidad, así como la explicación de la estructura de la memoria.
- **Capítulo 2: Planteamiento del trabajo** – Se describe la situación actual de este tipo de sistemas y el planteamiento del problema a resolver.
- **Capítulo 3: Estándar GSM** – Se detalla la parte teórica que su usa como base para el trabajo.
- **Capítulo 4: Recursos utilizados** – Se describen los elementos hardware y software usados en el desarrollo del trabajo.
- **Capítulo 5: Desarrollo del proyecto** – Se explica todo el procedimiento seguido en la realización del trabajo.
- **Capítulo 6: Pruebas y comprobaciones –** Se detallan todas las pruebas que se han hecho durante el trabajo y al final del mismo para comprobar que el resultado es el esperado.
- **Capítulo 7: Conclusiones** – Se exponen los resultados obtenidos, así como las futuras posibilidades de desarrollo.

1.2. English version

1.2.1. Motivation

Since its origin, telecommunication systems have worked out using a specific hardware for each function they perform. However, two decades ago the SDR (Software-Defined Radio) concept emerged. This concept refers to a radio system in which the specific hardware components are implemented by software through a general purpose processor.

In order to exploit the SDR platforms potential, the department of Signal Theory and Communications at the Carlos III University of Madrid has proposed different projects based on this technology. More specifically, this project appears to complement Isaac Morcillo's TFG [1], where a simple GSM [2] receiver is implemented in a SDR platform.

With the completion of this work we pretend to succeed in developing a part of GSM process. This work, together with other partners' projects, can serve as an example of these SDR platforms potential, which can simulate the complete GSM standard.

1.2.2. Objectives

The main objective of this work is to implement in a SDR platform the whole process that takes place when a mobile in a GSM network changes his zone and passes to be under the coverage of a new base station (BTS). This process, called "Location Update", involves sending and receiving a series of defined messages.

Therefore, the target is to create these messages from the beginning and follow the process that takes place in reality. This process includes the message coding according to the corresponding logical channel, the organization of these messages into frames, the GMSK modulation used in the standard and, on the part of the receiver, all the reverse process to get the original message.

As the main purpose of this paper is to illustrate a specific procedure, the synchronization process that is taken into GSM is not implemented strictly, so the sending and receiving of the messages will be done in a more direct way and without a rigorous synchronization.

Last, the main finality of this paper is simply to serve as an example for students of subjects related to mobile communications, so that they can do in the future some lab or work using the developed program.

1.2.3. Document structure

To make it easier for the reader and for a coherent reading, the memory is divided into seven chapters:

- **Chapter 1: Introduction** – The work motivation and his purpose are exposed, so as the explanation of the memory structure.
- **Chapter 2: Approach to work** – The current status of such kind of systems and the problem approach to be solved are described.
- **Chapter 3: GSM Standard** – It describes the theoretical part used at the developing of the work.
- **Chapter 4: Resources used** – It describes the hardware and software elements used in the work development.
- **Chapter 5: Project development** – It contains the explanation of the whole work realized.
- **Chapter 6: Checks and test** – It describes all the tests that have been made during the work development and at the end for proving that the result is as expected.
- **Chapter 7: Conclusions** – The results obtained and the future possibilities of development are exposed.

2. Planteamiento del trabajo

En este capítulo se expone la situación actual del marco tecnológico, socio-económico y regulador en el que se desarrolla el proyecto.

2.1. Estado del arte

2.1.1. Planteamiento del problema

Durante las últimas décadas hemos visto como la tecnología de las telecomunicaciones ha avanzado a pasos de gigante. Concretamente, el mundo de la telefonía móvil se vio revolucionado con la llegada en la década de los noventa del estándar GSM, el cual supuso una gran evolución.

Sin embargo, más adelante surgieron otros sistemas como UMTS [3], HSPA [4] o, el que se está impulsando más durante los últimos años, LTE [5]. Todos estos sistemas han ido mejorando las prestaciones y los servicios que se ofrecen al usuario, con el fin de adaptarse a las condiciones que se han ido imponiendo con el tiempo.

Por otro lado, el desarrollo de los computadores ha permitido que muchas de las tareas que hasta hace no mucho se realizaban gracias a un hardware específico, puedan realizarse mediante software. En el caso de los sistemas radio, esta forma de implementación se denomina SDR [6].Estos sistemas requieren básicamente un conversor analógico-digital y un adaptador de radiofrecuencia. Las plataformas SDR también han evolucionado con el tiempo, aunque en la actualidad no se usan para suplir los sistemas radio tradicionales, ya que estos son, por lo general, más rápidos y eficientes. Sin embargo, las ventajas que ofrece la plataforma no son pocas, siendo la más interesante la posibilidad de desarrollar muchos de los distintos sistemas de comunicaciones que existen sin necesidad de un hardware muy específico. Es por eso que en este trabajo se va usar una plataforma SDR que permita implementar mediante software el procedimiento deseado.

De forma concreta, las herramientas que se van a usar para desarrollar el trabajo son de la empresa National Instruments, ya que son las que están disponibles en la universidad. El software usado es LabVIEW [7], que constituye una completa herramienta de desarrollo para multitud de sistemas de ingeniería. En cuanto al hardware, se usará el transceptor USRP-2920 [8], cuyas funciones se detallarán en el capítulo 4.

2.1.2. Alternativas

Como hemos visto, las herramientas que se usan en el trabajo son de la empresa National Instruments, aunque también existen otras plataformas SDR que podrían utilizarse.

2.1.2.1. GNU Radio

GNU Radio [9] es un conjunto de herramientas software gratuitas que permiten el procesado de señales sin necesidad de hardware especializado, ya que es compatible con procesadores de uso general y elementos hardware de radiofrecuencia de bajo coste.

Por tanto, podría usarse con elementos como el USRP de National Instruments u otros transceptores más asequibles. También puede usarse como complemento de otras herramientas software gratuitas como GNU Octave [10] o de pago como MATLAB [11].

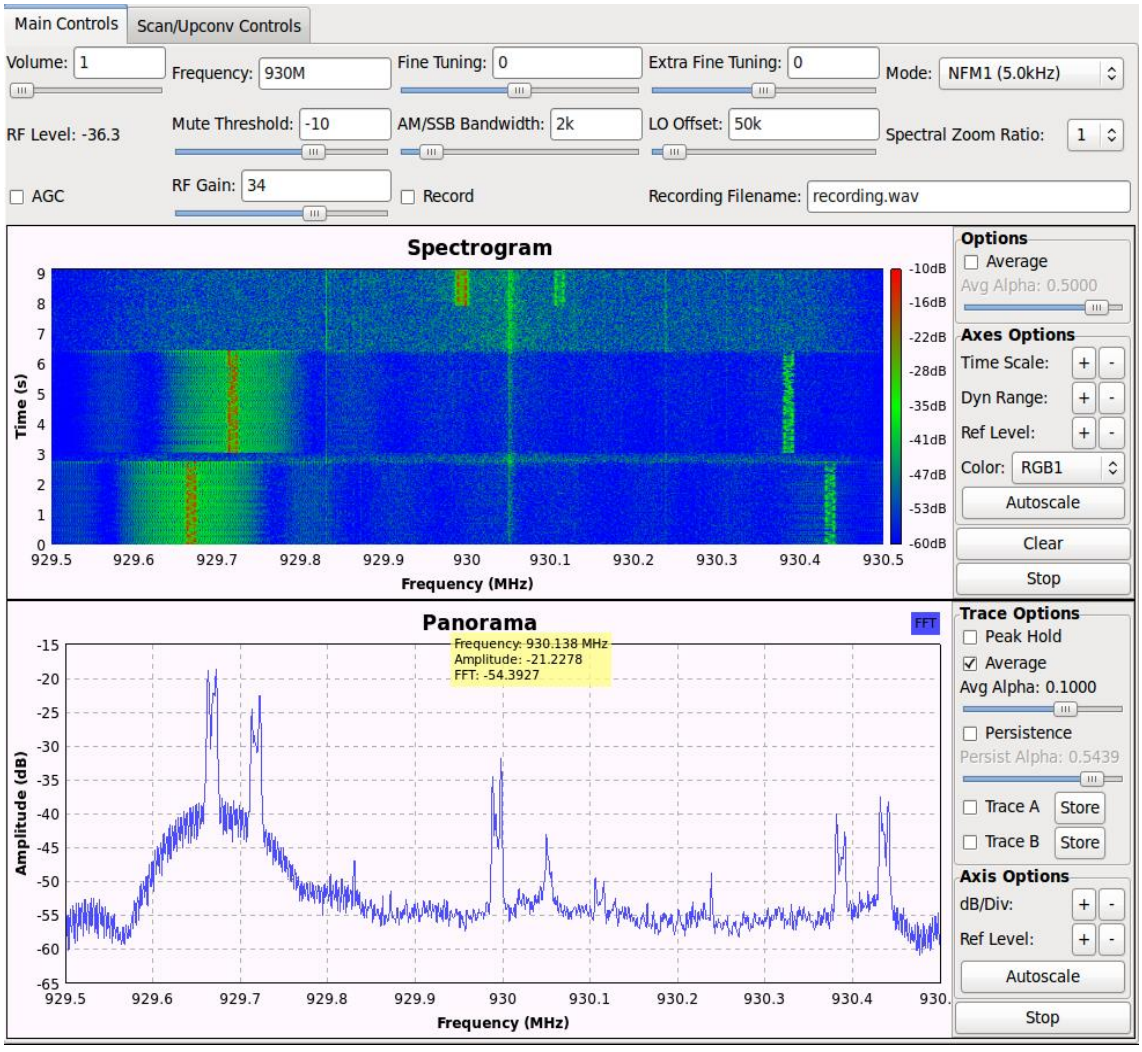

Figura 1: Herramienta SDR GNU Radio

2.1.2.2. SDR-RADIO.com

SDR-RADIO.com [12] es una herramienta gratuita para Windows que provee una potente interfaz gráfica para los usuarios de las plataformas SDR.

Esta herramienta soporta tanto receptores como transceptores adaptados al SDR y, al igual que en el caso de GNU Radio no requiere de un computador demasiado avanzado para funcionar de forma correcta.

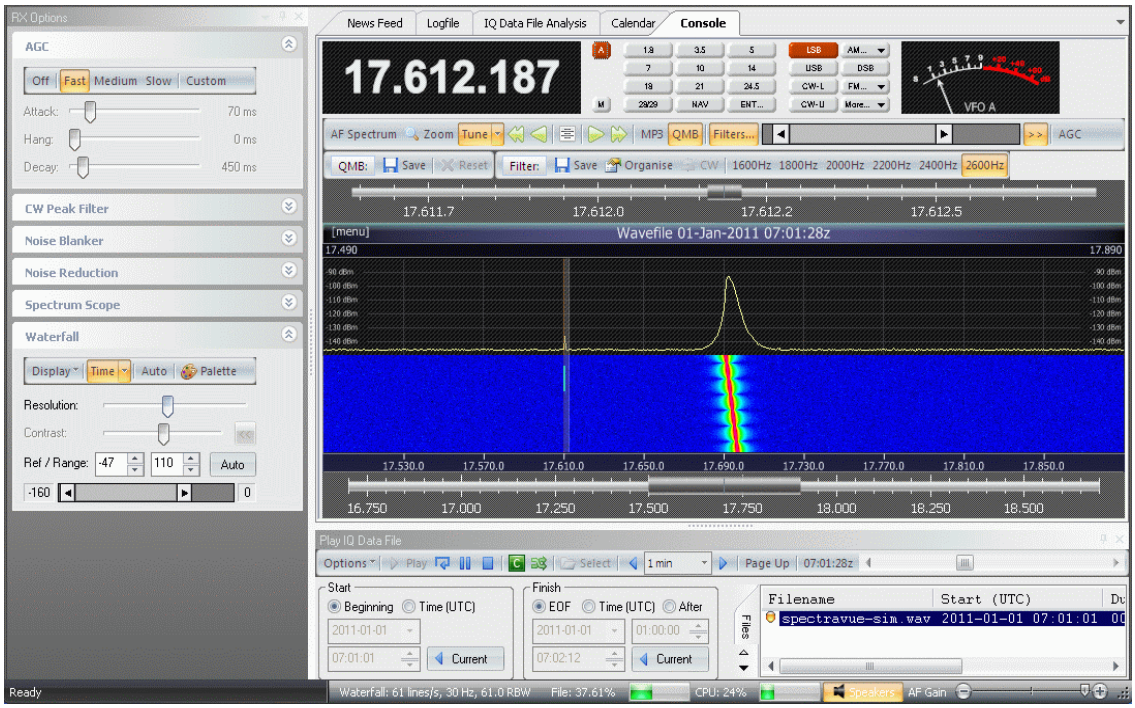

Figura 2: Herramienta SDR-RADIO.com

2.1.3. Conclusiones

Como hemos visto hay diversas posibilidades para implementar este trabajo en una plataforma SDR (resumen en la Tabla 1). Aunque la elección de alguna de las herramientas gratuitas que se han expuesto pudiera reducir los costes del trabajo, la decisión de utilizar el software LabVIEW de National Instruments se debe a que se trata de una herramienta muy completa que se ajusta completamente a las necesidades del trabajo. Además, como estudiante de la Universidad Carlos III de Madrid, la empresa proporciona una licencia de estudiante para poder usar el programa.

Software	Coste	Integración del NI USRP-2920	Sistema Operativo	Carga computacional
LabVIEW	2920€ - Sin coste para el estudiante	Muy alta	Windows GNU/Linux OS X	Media
GNU Radio	Gratuito	Media	Windows GNU/Linux OS X	Baja
SDR-RADIO.com	Gratuito	Media	Windows	Baja

Tabla 1: Alternativas software

En cuanto al hardware, la elección de los equipos de National Instruments es directa, ya que son los equipos que están disponibles en el laboratorio del departamento y cumplen con los requisitos necesarios.

2.2. Entorno socio-económico

En cuanto al entorno socio-económico en el que se enmarca este trabajo, no hay aspectos que hayan afectado de forma directa al desarrollo del mismo. Sin embargo, sí que puede considerarse que en un futuro implicará una mejora de la sociedad, ya que es un trabajo que tiene como finalidad ser usado como material docente y, por tanto, puede conseguir que esta docencia sea mejor y más práctica. De esta forma se trata de conseguir que los futuros ingenieros estén mejor preparados y tengan conocimientos más prácticos de un tema concreto y de gran actualidad y futuro como el de las comunicaciones móviles.

Por otro lado, para ver el coste económico que ha supuesto el desarrollo de este proyecto, se adjunta en el anexo B un presupuesto detallado.

2.3. Marco regulador

El proyecto se encuentra enmarcado en un entorno específico al que debe adaptarse para cumplir con todas las restricciones existentes. Dentro de estas restricciones podemos diferenciar de dos tipos: legales y técnicas.

2.3.1. Marco legal

En cuanto al marco legal, al tratarse de un trabajo que se realiza dentro de la universidad y sin finalidad de usar los resultados fuera de ella, no hay restricciones legales relevantes que le afecten de forma directa. Sin embargo, como todas las obras, está sujeto a la Ley de Propiedad Intelectual, la cual constituye el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación [13]. Por otro lado, las leyes que más pueden afectar al desarrollo del TFG tienen que ver con la transmisión de señales radioeléctricas y están expuestas en el siguiente apartado.

2.3.2. Marco técnico

Respecto al marco técnico, sí podemos considerar más restricciones, las cuales vienen definidas par la Ley 9/14, de 9 de mayo, General de Telecomunicaciones [14], y el Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas [15].

No obstante, en ningún momento durante la realización del trabajo se incumplen las restricciones que en los documentos anteriormente citados se detallan, ya que todos los equipos del laboratorio cumplen con la normativa vigente. En el caso del trabajo realizado se hace uso del transceptor USRP-2920, este dispositivo por sus características técnicas (potencia máxima de 100mW a las frecuencias usadas en el proyecto) [16] no puede alcanzar en ningún caso los valores máximos permitidos.

3. Estándar GSM

Con el fin de contextualizar el trabajo realizado, y para poder entender lo que en él se realiza, es conveniente exponer una visión extendida del estándar GSM en el que se basa. Aunque no todo lo que se explica afecte directamente al desarrollo del trabajo, sí es necesario tenerlo en cuenta para comprender el funcionamiento global del mismo.

3.1. Introducción

3.1.1. Historia

El estándar GSM comenzó a desarrollarse en 1982 a raíz de la conferencia del CEPT (*Conférence européenne des administrations des postes et des télécommunications*) de ese año, en la que se creó el *Groupe Spécial Mobile*, cuyo objetivo era el de crear un estándar europeo de comunicaciones móviles digitales. La decisión de desarrollar este estándar común en toda Europa se tomó para conseguir un sistema válido en todo el territorio, evitando así los problemas de compatibilidad que se habían dado con otros sistemas anteriores.

Dos de las decisiones más importantes que se llevaron a cabo fueron la reserva de una banda de frecuencia común en toda Europa (890-915 / 935-960 MHz) y el desarrollo e implantación por fases del sistema, permitiendo ofrecer un sistema básico que fuera creciendo para añadir funcionalidades con el tiempo.

En 1990 ya se finalizó el primer estándar GSM-900 y fue un año más tarde cuando ocurrió lo mismo con el estándar DCS-1800 (una ampliación de GSM en la banda de 1800 MHz). Sin embargo, hasta 1992 no iniciaron su actividad las primeras redes GSM-900 ni se fabricaron los primeros equipos comerciales. A partir de ese momento, GSM fue ganando terreno por todo el mundo para convertirse en el estándar más usado de la telefonía móvil, y fue el sistema predominante hasta la llegada en 2001 de UMTS que, aunque lentamente, fue desplegándose y ofreciendo mayores prestaciones.

3.1.2. Servicios

Los servicios ofrecidos por GSM se pueden dividir en tres tipos, que fueron desplegados en dos fases:

- Teleservicios
  - Fase I
    - Telefonía Full Speed (13 kbps).
    - Llamadas de emergencia (voz).
    - Mensajes cortos (SMS).
  - Fase II
    - Telefonía Half Speed (6.5 kbps).
    - SMS mejorado.

- Servicios portadores
  - Fase I
    - Datos asíncronos en modo circuito.
    - Datos síncronos en modo circuito.
    - Acceso PAD (Packet Assembly - Disassembly) asíncrono.
  - Fase II
    - Acceso PAD dedicado.
    - Acceso en modo paquete dedicado síncrono.
- Servicios suplementarios
  - Fase I
    - Desvío de llamadas.
    - Restricción de llamadas.
  - Fase II
    - Identificación de línea llamante.
    - Llamada en espera.
    - Retención de llamada.
    - Multiconferencia.
    - Restricción de servicios por el operador.

3.1.3. Sistema celular

Para poder ofrecer los servicios que se plantean en GSM se decidió que lo mejor era usar un sistema celular, este sistema ofrece grandes prestaciones de cobertura, capacidad y aprovechamiento del espectro.

El fundamento de los sistemas celulares se basa en la división de la superficie en la que se quiere dar servicio en celdas o células, en las cuales se encuentra la antena encargada de realizar la comunicación con los terminales móviles.

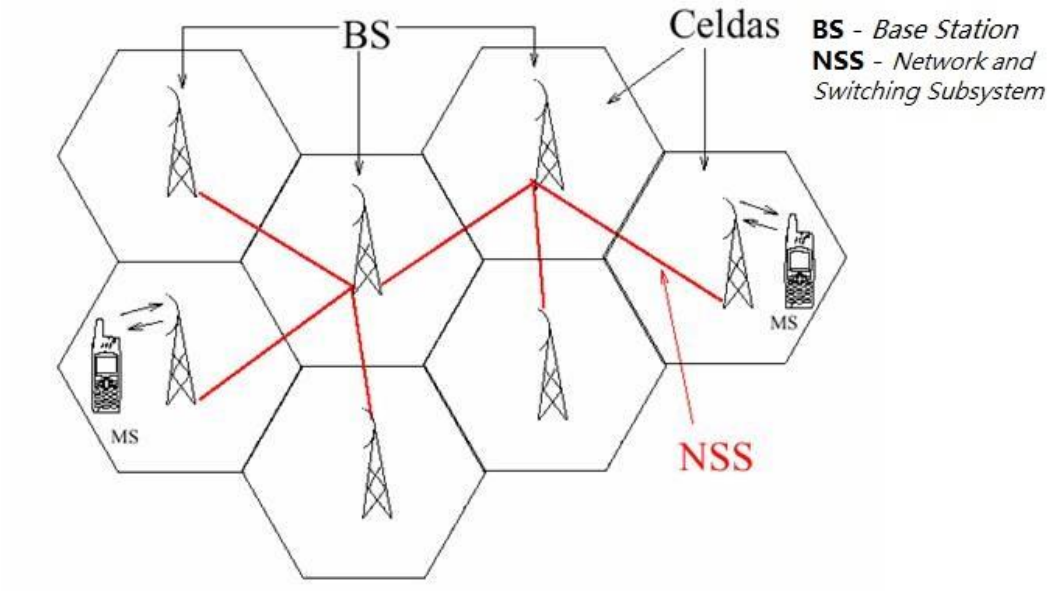

Figura 3: Sistema celular [17]

Esta división ofrece múltiples ventajas como:

- **La capacidad de la red aumenta**, ya que las frecuencias disponibles se pueden reutilizar en las distintas celdas, de forma que varios usuarios puedan usar la misma frecuencia pero al estar separados suficiente distancia no existe una interferencia reseñable.
- **Reducción del uso de energía**, debido a que las antenas, al cubrir zonas más pequeñas, requieren menos energía.
- **Mayor flexibilidad en la planificación**, ya que dependiendo de las características de la zona en la que se quiere ofrecer el servicio, es posible dimensionar la red de la forma que mejor se adapte a las necesidades específicas.
- **Evolución gradual**, facilitando la expansión de la red si fuera necesario.

Sin embargo, el sistema celular es un sistema limitado por interferencia, esto es debido a que la reutilización de frecuencias conlleva la necesidad de una planificación adecuada, de manera que ninguna celda use la misma frecuencia que su adyacente. Si esto ocurriera la interferencia entre ambas celdas sería muy alta y no permitiría dar un buen servicio. La distancia mínima para evitar interferencias que debe haber entre dos celdas que usan la misma frecuencia se denomina distancia cocanal.

Por lo general, las celdas de los sistemas celulares están diseñadas de forma hexagonal con una antena omnidireccional en el centro de la misma. Esto es debido a que dentro de las formas poligonales que cumplen con la condición de cubrir un área sin solapes (también lo cumplen los cuadrados y los triángulos), el hexágono cubre mayor superficie con el mismo rango de cobertura. Sin embargo, con el aumento de la demanda surgió el concepto de la sectorización, que en lugar de hacer uso de antenas omnidireccionales en el centro de las celdas, consiste en colocar antenas directivas en los extremos. De esta forma se consigue reducir las interferencias y, por tanto, reducir la distancia cocanal y aumentar la reutilización de frecuencias.

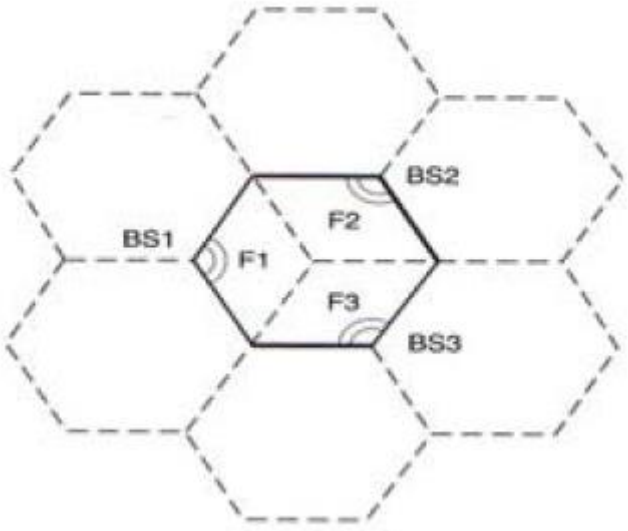

Figura 4: Ejemplo de sectorización [18]

3.2. Arquitectura

Como se ha mencionado antes, GSM es un sistema celular que, debido a su complejidad, se agrupa en subsistemas o conjuntos de equipos (ilustrados en la Figura 5) que realizan una tarea específica. Estos subsistemas se dividen en tres tipos:

- Subsistema de estación base BSS (*Base Station Subsystem*).
- Subsistema de red NSS (*Network and Switching Subsystem*).
- Subsistema de operación y mantenimiento OSS (*Operation Support Subsystem*).

Además de estos tres subsistemas encontramos la estación móvil MS (*Mobile Station*).

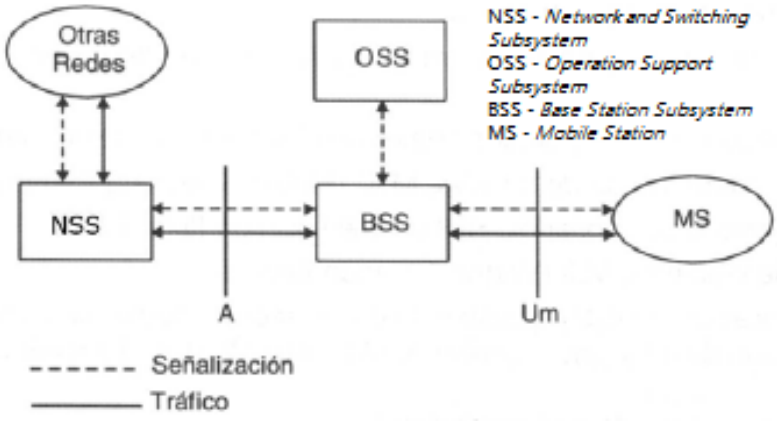

Figura 5: Estructura de la red GSM [19]

A continuación se detallan los componentes y las principales funciones de los subsistemas de GSM más importantes.

3.2.1. Estación Móvil (MS)

Está formada por dos elementos:

- **Parte de usuario**: tarjeta inteligente SIM (*Subscriber Identity Module*), que contiene los datos que el sistema necesita conocer del usuario, como claves y algoritmos de identificación y cifrado o identificativos como el IMSI (*International Mobile Subscriber Identity*) y el TMSI (*Temporary Mobile Subscriber Identity*).
- **Parte de equipo**: equipo terminal que realiza las funciones de proceso y radio para acceder al sistema y contiene un número de identificación único denominado IMEI (*International Mobile Equipment Identity*).

Sus funciones principales son:

- Interfaz de comunicación entre el usuario y la red radio.
- Transmisión y recepción de la información del usuario y de la señalización en la interfaz radio.
- Sintonización de frecuencias y seguimiento automático de las estaciones base.

- Iniciación de la conexión con la red.
- Procesado de voz.
- Adaptación de interfaces y velocidades para señales de datos.

Figura 6: Mobile Station [20]

3.2.2. Subsistema de Estación Base (BSS)

Este subsistema engloba dos elementos:

- **Transceptores de estación base, BTS (*Base Transceiver Station*)**: encargados de la transmisión y la recepción (dispositivos radio y de proceso digital).
- **Controladores de BTS, BSC (*Base Station Controller*)**: controlan los recursos radio de uno o varios BTS y conectan con la central de conmutación móvil.

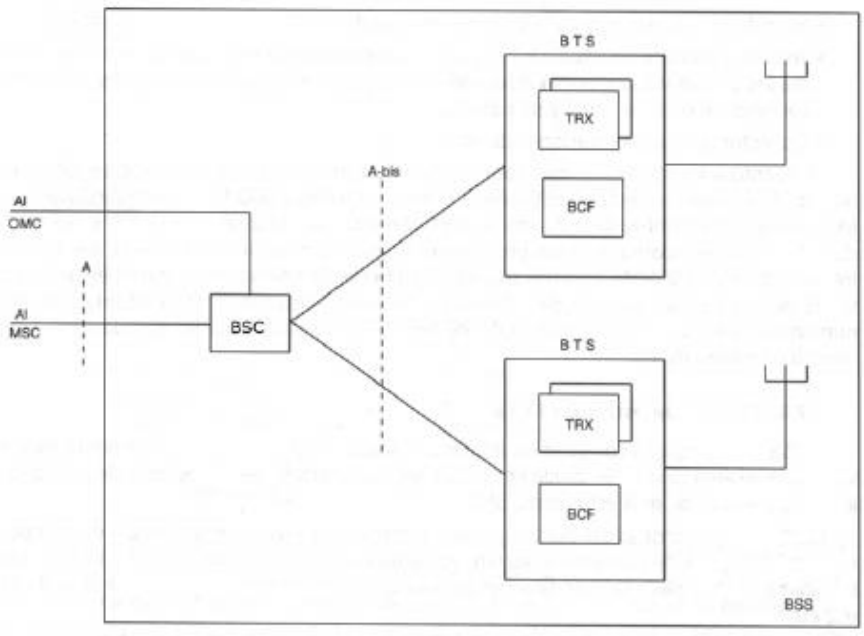

Figura 7: Arquitectura del subsistema BSS [19]

En cuanto a las funciones que se realizan en este subsistema destacan:

- Transmisión y recepción radioeléctrica.
- Localización de la estación móvil para el registro inicial o la actualización.
- Establecimiento, supervisión y conclusión de llamadas.
- Procesado de voz y adaptación de velocidades.
- Control de equipos y funciones de reconfiguración.
- Control del mantenimiento rutinario.

3.2.3. Subsistema de Red (NSS)

Este subsistema es el más complejo en cuanto a elementos ya que representa el núcleo de la red y se encarga de su control. Está formado por:

- **Centro de conmutación móvil, MSC (*Mobile services Switching Centre*)**: se trata de una central telefónica de la que dependen uno o varios BSC con funciones de conmutación adicionales para tener en cuenta la movilidad de los usuarios. También realiza otras funciones como:
  - Procedimientos para la localización y registro de abonados y su actualización.
  - Gestión de llamadas y aviso a la estación móvil de las llamadas entrantes.
  - Procedimientos para el traspaso de llamadas.
  - Funciones de "pasarela" para comunicarse con la PSTN (*Public Switched Telephone Network*) a través del GMSC (*Gateway Mobile services Switching Centre*).
  - Recopilación de datos de tráfico y facturación.
- **Registro de usuarios, HLR (*Home Location Register*)**: es la base de datos donde están registrados todos los clientes de un operador. Por lo general existe un único HLR por red GSM y todas las llamadas entrantes convergen en él. Consta de dos tipos de datos:
  - Datos permanentes: Identificación y números del abonado y la red, estos son el IMSI y el número de teléfono MSISDN (*Mobile Station Integrated Services Digital Network*)
  - Datos temporales: tales como el número de localización itinerante MSRN (*Mobile Subscriber Roaming Number*), la dirección VLR y la localización de la MSC en la que se encuentra el usuario.
- **Registro de usuarios visitantes, VLR (*Visitor Location Register*)**: es la base de datos asociada a una MSC con información de los usuarios activos en esa MSC. El VLR obtiene la información para poder gestionar las llamadas del HLR. Los datos que almacena el VLR son el IMSI, el TMSI, el MSISDN, el número de encaminamiento MSRN (*Mobile Subscriber Roaming Number*) y la identidad de la zona de localización LAI (*Location Area Identification*). Por lo general existe un VLR por cada MSC y todo abonado activo debe estar inscrito en uno.

- **Centro de autenticación, AuC (*Authentication Centre*)**: guarda las identidades IMSI y la clave de identificación secreta de cada usuario. Está asociado al HLR y proporciona al sistema la información necesaria para la autentificación de los usuarios.
- **Base de datos de equipos, EIR (*Equipment Identity Register*)**: contiene las identidades de los equipos móviles (IMEI) clasificados en tres listas:
  - Lista blanca: equipos homologados.
  - Lista gris: equipos que es necesario localizar.
  - Lista negra: equipos robados o defectuosos que no pueden acceder a la red.

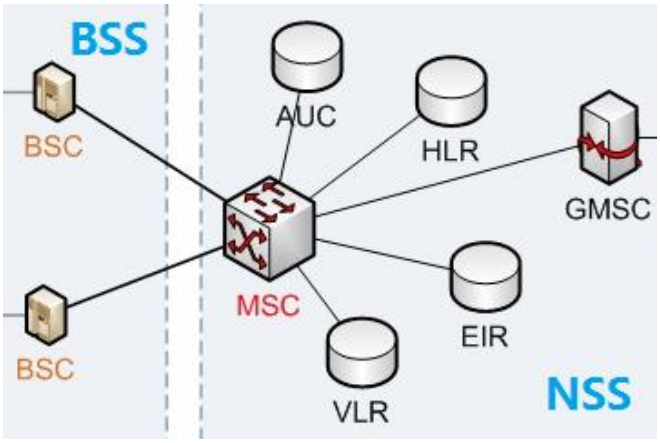

Figura 8: Arquitectura del subsistema NSS [21]

3.3. Interfaz radio

La interfaz radio constituye el nivel físico de GSM, y está regido por una serie de procedimientos que indican el modo de utilización de los recursos radio de los que se disponen. Estos procedimientos son de gran interés en el trabajo realizado, ya que todo el desarrollo del mismo está basado en la interfaz radio, y por tanto se usan muchos de los métodos y normas que se exponen a continuación.

3.3.1. Multiacceso en GSM

La interfaz radio de GSM combina el acceso por división en frecuencia (FDMA/FDD) con el acceso por división en el tiempo (TDMA), lo que significa que una misma portadora se comparte en tiempo por varios usuarios, en este caso cada trama TDMA se divide en 8 intervalos. Cada uno de los intervalos de denomina *timeslot* y van del TN0 al TN7, usándose el TN0 para la conexión y el control de las estaciones móviles. A su vez, los radiocanales están separados 200 kHz entre sí.

Esta división en tiempo y frecuencia se realiza para conseguir los timeslots, cada uno de los cuales corresponde a un canal físico, y es válida tanto en los enlaces ascendentes (MS - BTS) como en los descendentes (BTS - MS). Sin embargo, entre los enlaces ascendente y descendente existe un desplazamiento temporal de 3 intervalos entre el mismo timeslot de subida y bajada, de esta forma, aunque cuando se establece un canal se usa el mismo timeslot, se evita el tener que emitir y recibir al mismo tiempo.

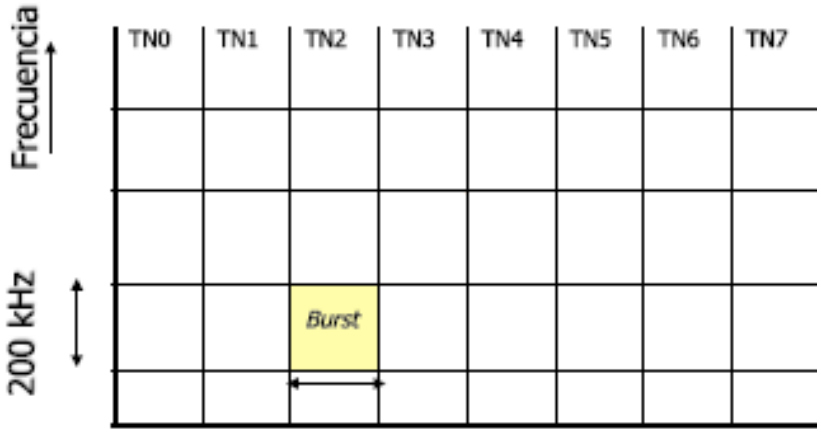

Figura 9: Acceso FDMA/TDMA en GSM [22]

La secuencia de bits que se transmite en un timeslot se denomina ráfaga o *burst*, esta secuencia consta generalmente de 148 bits más un periodo de guarda correspondiente a 8.25 bits. Por lo tanto, teniendo en cuenta que el tiempo de transmisión de un bit es de 0.577 ms, la velocidad de transmisión radio es de 156.25 bits/0.577 ms = 270,833 kbps.

Existen varios tipos de ráfagas según su contenido y estructura:

- **Ráfaga normal (NB, *Normal Burst*)**

Se usa para la transmisión de canales de tráfico y de control, es el tipo de ráfaga más común (Figura 10).

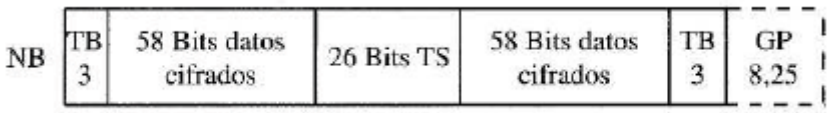

Figura 10: Normal Burst [22]

- **Ráfaga de corrección de frecuencia (FB, *Frequency correction Burst*)**

Se utiliza para la sincronización de la frecuencia de la estación móvil (Figura 11).

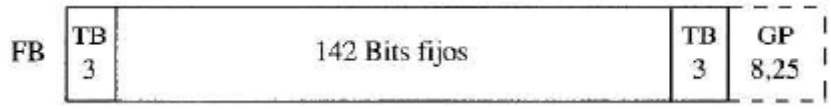

Figura 11: Frequency correction Burst [22]

- **Ráfaga de sincronización (SB, *Synchronization Burst*)**

Sirve para la sincronización en el tiempo de la estación móvil (Figura 12).

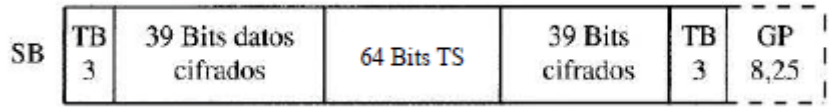

Figura 12: Synchronization Burst [22]

- **Ráfaga de relleno (DB, *Dummy Burst*)**

Sirve para rellenar la transmisión cuando hay canales de tráfico vacíos. Está formada por una serie de bits conocidos (Figura 13).

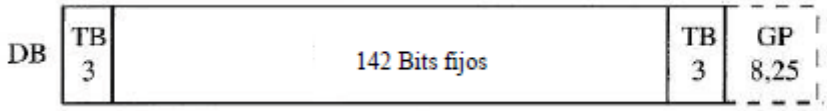

Figura 13: Dummy Burst [22]

- **Ráfaga de acceso (AB, *Access Burst*)**

Es la ráfaga utilizada para acceder al sistema, en ella se transmite el RACH y se caracteriza por su gran periodo de guarda de 68.25 bits (Figura 14).

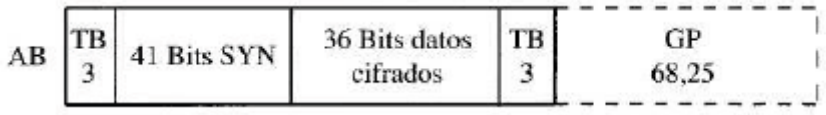

Figura 14: Access Burst [22]

En cuanto a la organización de las ráfagas ya hemos visto como estas van contenidas en un timeslot y como la unión de 8 timeslots da lugar a una trama. Sin embargo, las tramas también se agrupan entre sí antes de ser enviadas por el canal de radio, de forma que se permiten uniones de 26 y de 51 tramas denominadas MF26 y MF51. Las MF26 se utilizan típicamente para los canales de tráfico, mientras que las MF51 se usan para los canales de señalización.

A su vez estas MF26 y MF 51 se agrupan en supertramas, las cuales contienen 51 MF26 o 26 MF51, dando lugar a un total de 1326 tramas en ambos casos. Por último están las hipertramas, que contienen 2048 supertramas, lo que supone un total de 2715648 tramas.

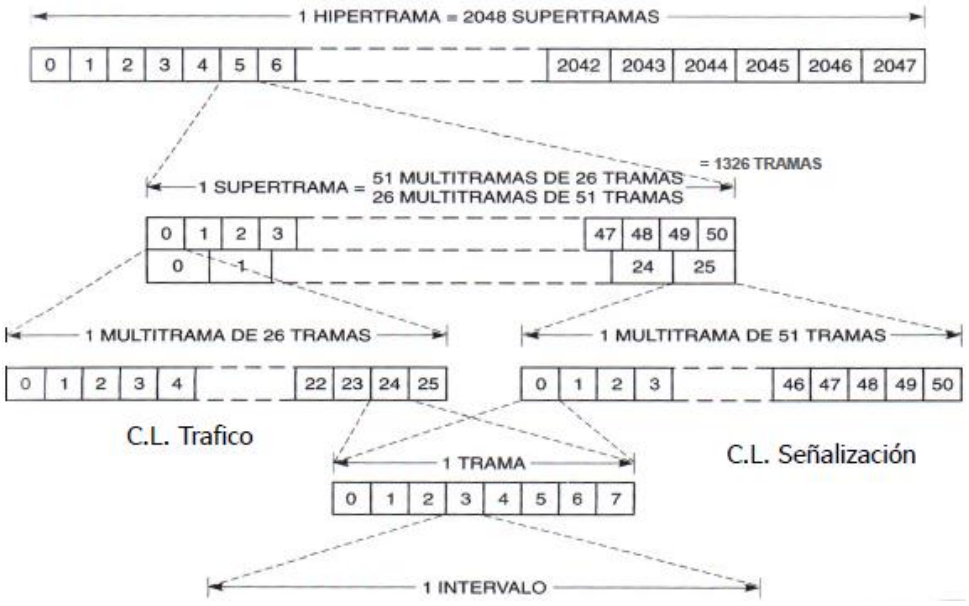

Figura 15: Jerarquía de tramas [22]

3.3.2. Canales físicos y lógicos

Como se ha explicado en el apartado anterior, un canal físico en GSM corresponde a un intervalo de tiempo o timeslot. No obstante, los distintos tipos de información que se envían a través de los canales físicos se denominan canales lógicos.

Existen dos tipos de canales lógicos: los canales de tráfico y los de control.

Canales de tráfico TCH (*Traffic Channel*)

Los canales de tráfico son los usados para llevar tanto el tráfico de voz como el de datos. Dentro de los canales de tráfico hay de cuatro tipos según la velocidad de transmisión y la clase de información que llevan:

- **Velocidad total TCH/FS (*TCH Full rate Speed*)**:
  - 13 Kbit/s en voz.
  - 9,6 Kbit/s en datos.
- **Velocidad mitad TCH/HS (*TCH Half rate Speed*)**:
  - 6,5 Kbit/s en voz.
  - 4,8 Kbit/s en datos.

Canales de control CCH (*Control Channel*)

Los canales de control se utilizan para las funciones de señalización y otras funciones especiales como los mensajes cortos. Estos canales se pueden dividir en dos tipos:

- **Canales de control comunes**, regulan el acceso de los terminales al sistema. Estos canales se subdividen en dos grupos:
  - **BCH (*Broadcast Control Channel*)**: ↓[1], difunden información general de la red, de la célula actual y de las adyacentes, así como parámetros del sistema y ráfagas de sincronización. Hay tres tipos de canales BCH:
    - **BCCH (*Broadcast Common Control Channel*)**: transmite información general de la BTS y la configuración de otros canales de control.
    - **FCCH (*Frequency Correction Channel*)**: transmite la señal piloto para el ajuste de la frecuencia en las estaciones móviles.
    - **SCH (*Synchronization Channel*)**: transmite la información para la sincronización de trama (identificación de posición) e identificación de la estación base (BSIC, *Base Station Identity Code*).
  - **CCCH (*Common Control Channel*)**: existen tres diferentes:
    - **RACH (*Random Access Channel*)**: ↑[2], canal por el que se cursan las peticiones no programadas de la estación móvil a la red.
    - **PCH (*Paging Channel*)**: ↓, encargado de notificar a la estación móvil que existe una llamada destinada a la misma.

[1] ↓ Usado en el enlace descendente
[2] ↑ Usado en el enlace ascendente

        - **AGCH (*Access Grant Channel*)**: ↓, canal encargado de asignar recursos (SDCCH, TCH) al móvil que previamente solicitó el establecimiento de la comunicación (generalmente a través del RACH).
- **Canales de control dedicados**, son los encargados de transmitir la señalización asociada a las llamadas. Existen tres canales de control dedicados:
    - **SDCCH (*Stand Alone Dedicated Control Channel*)**: ↑↓, se utiliza para el intercambio de datos entre la estación móvil y la estación base antes de asignar un canal de tráfico.
    - **SACCH (*Slow Associated Control Channel*)**: ↑↓, se utiliza para transmitir la señalización general asociada a la llamada mientras se produce la conversación.
    - **FACCH (*Fast Associated Control Channel*)**: ↑↓, se utiliza para transmitir la señalización de ordenes urgentes (como el traspaso) durante la llamada. Este canal usa parte de los bits del canal de información.

Por otra parte nos encontramos con el CBCH (*Cell Broadcast Channel*) que es un canal independiente de los anteriores y sirve para difundir mensajes cortos desde una célula.

3.3.3. Procesado en banda base

Todos los datos que se quieren enviar en GSM pasan por un proceso en el que se tratan y se preparan para poder ser enviados por el canal radio. Los pasos que se siguen en este procedimiento son los siguientes:

- **Codificación de fuente** (para canales de voz).
    - Tiene como objetivo minimizar la cantidad de información que se quiere transmitir para un nivel de calidad determinado.
    - Se reduce cada muestra de 20 ms de voz (que originalmente consta de 160 muestras con 13 bits cada una) a 260 bits.
    - Se usa una codificación predictiva lineal RPE-LPT (*Regular Pulse Excited – Long Term Prediction*).
- **Codificación de canal** (para canales de tráfico y de señalización).
    - Se realiza con el objetivo de detectar y corregir errores que se puedan producir en la transmisión.
    - Se introduce redundancia para minimizar los desvanecimientos producidos por el canal radio.
    - Se utilizan códigos bloque y convolucional para corregir errores, códigos FIRE para su detección y la corrección de errores "de ráfaga" (agrupados) y códigos de paridad para detección.
    - Tras esta codificación lo usual es que resulten secuencias de 456 bits.
- **Entrelazado**
    - Se distribuyen las secuencias de bits que resultan de la codificación de manera no consecutiva en las tramas TDMA.

- Se realiza para evitar que los errores que pueda introducir el canal radio no afecten a bits consecutivos.

Concretamente, podemos ver cómo cambia la codificación de canal según el tipo de datos que se van a transmitir.

Para los canales de tráfico (voz), se lleva a cabo una codificación que convierte los 260 bits, correspondientes a 20 ms de voz digitalizada que salían de la codificación de fuente, en 456 bits, que serán los que pasen al siguiente proceso. Esta codificación se lleva a cabo en los siguientes pasos (ilustrados en la Figura 16):

- Se clasifican los 260 bits en tres clases según su importancia, esto da lugar a 50 bits de la clase 1A (los más importantes), 132 bits de la clase (los intermedios) y 78 bits de la clase 2 (los menos importantes).
- Los bits de la clase 1A pasan por un código bloque (53,3) dando lugar a 53 bits.
- Estos 53 bits junto con los bits de la clase 1B y 4 bits de cola (189 bits en total) pasan por un codificador convolucional 1/2, dando lugar a 378 bits.
- A continuación se añaden los bits de la clase 2, que van sin protección, y el resultado son los 456 bits de salida.

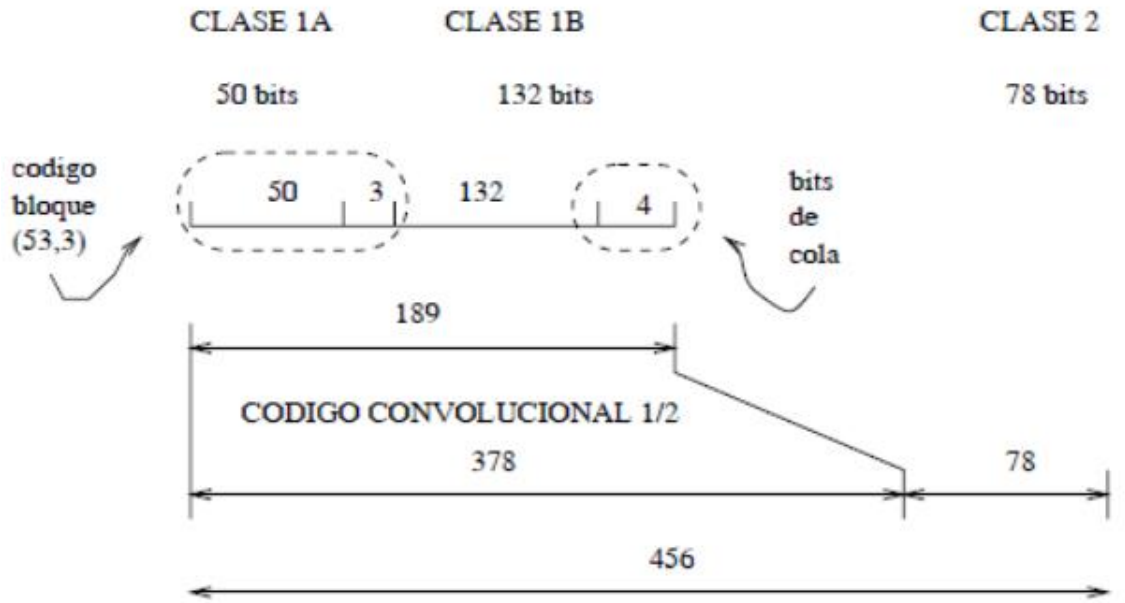

Figura 16: Proceso de codificación de un canal de tráfico (voz) [22]

De la misma manera, los canales de control tienen su propia codificación que convierte 184 bits en 456. Esta codificación se lleva a cabo en los siguientes pasos (ilustrados en la Figura 17):

- Los 184 bits pasan por un código FIRE del que resultan 224 bits.
- A estos bits se les añaden 4 bits de cola.
- Los 228 bits resultantes pasan por un código convolucional 1/2, lo que da como resultado los 456 bits de salida.

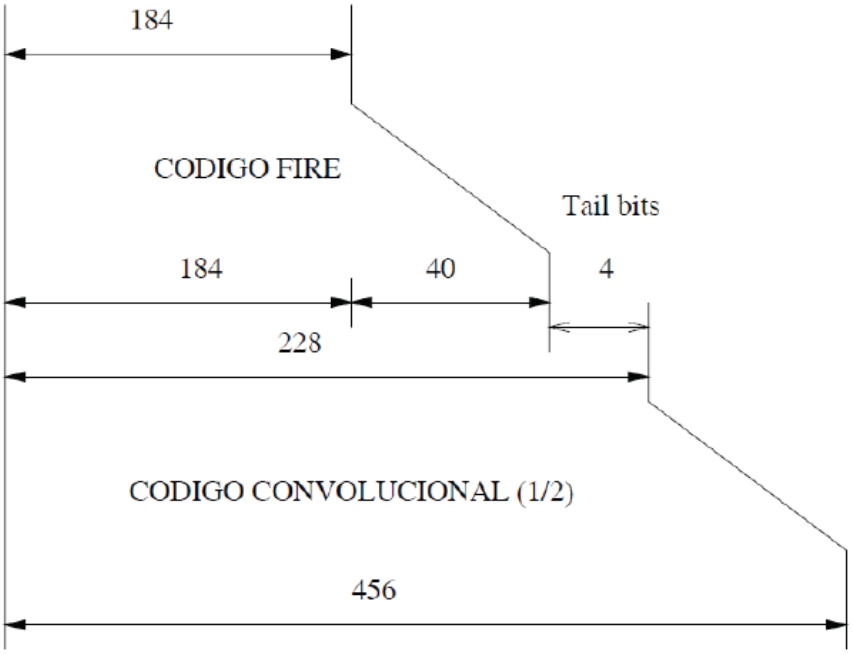

Figura 17: Proceso de codificación de un canal de control [22]

Tanto en la codificación del canal de tráfico (voz) como en la codificación del canal de control se realiza al final una división de los 456 bits que resultan. En el caso del canal de voz, estos bits se dividen en 8 sub-bloques de 57 bits (correspondiente a la mitad de los datos que admite una Normal Burst) qué, junto con los sub-bloques de otros cinco canales de voz pasarán por el proceso de entrelazado antes de ser enviados. Sin embargo, en el caso del canal de control, el entrelazado se realiza en cuatro tramas completas, ya que los 456 bits se dividen en cuatro grupos de 114 bits que se reparten en cuatro Normal Burst.

3.3.4. Modulación

En cuanto a la modulación, en GSM se utiliza una modificación de la modulación MSK (*Minimum Shift Keying*) que se denomina GMSK (*Gaussian Minimum Shift Keying*). Se trata de una modulación por desplazamiento de fase con la peculiaridad de que, antes de pasar al circuito modulador, el flujo de datos pasa por un filtro pasobajo gaussiano, lo que permite suavizar las transiciones de fase de la señal, de forma que el nivel de los lóbulos secundarios producidos se reduce. La modulación GMSK, por tanto, tiene los siguientes objetivos:

- Alta eficiencia espectral.
- Baja radiación en los canales adyacentes.
- Continuidad de fase.
- Envolvente de la señal modulada contante.
- Modulador y demodulador sencillos.

Sin embargo, esta modulación presenta un inconveniente, y es que la duración del pulso a la salida del filtro es superior al tiempo de bit, lo que puede provocar interferencia entre símbolos.

4. Recursos utilizados

Como ya se comentó en el capítulo 2, la plataforma SDR utilizada está compuesta por los transceptores NI USRP-2920 y el programa LabVIEW. Sin embargo, también se han utilizado otros recursos para la realización del trabajo. En este capítulo se explicarán en detalle todos los elementos usados en el proyecto.

Además, todos los equipos especializados utilizados se encontraban en el laboratorio de comunicaciones móviles de la Universidad Carlos III de Madrid, situado en el edificio Torres Quevedo de la Escuela Politécnico Superior (campus de Leganés).

4.1. Transceptor NI USRP-2920

El transceptor USRP-2920 de National Instruments [8] es un aparato destinado al uso práctico para la enseñanza, ya que junto al software LabVIEW permite crear una importante plataforma SDR para la experimentación de las comunicaciones móviles en múltiples bandas de frecuencia.

Figura 18: Transceptor NI USRP-2920 [8]

Las características más interesantes de estos transceptores para la realización del proyecto son las siguientes:

- Frecuencia ajustable desde 50 MHz hasta 2.2 GHz, en el caso de este trabajo se utiliza la frecuencia de 600 MHz para el enlace ascendente y 645 MHz para el enlace descendente.

- Hasta 20 MHz de banda base I/Q con transmisión de hasta 25 MS/s para procesamiento basado en servidores con NI LabVIEW. En el caso de este trabajo se requiere un ancho de banda instantáneo de 200 KHz (un canal GSM) y se transmite con una tasa de 1,083 Mmuestras/s (cuatro muestras por cada símbolo en GSM).

Además, estos transceptores ofrecen la posibilidad de conectarse entre sí a través de un cable MIMO, de forma que con un solo ordenador se pueden controlar dos aparatos. Gracias a esto se ha podido realizar el trabajo, ya que durante gran parte de las pruebas se ha utilizado un transceptor como emisor y otro como receptor, controlados ambos por el mismo

ordenador. Sin embargo, durante las pruebas finales fue necesario el uso de cuatro transceptores y dos ordenadores, esto es debido a que el programa final se divide en dos partes, una correspondiente a la estación móvil y otra correspondiente a la estación base, de forma que cada ordenador se encarga de controlar dos transceptores, usándose uno para recibir y otro para enviar. Hacer esto es necesario porque los transceptores no son capaces de realizar con solvencia la emisión y la recepción en distintas frecuencias al mismo tiempo.

Por otro lado, tanto para la emisión como para la recepción, se utiliza una antena conectada al puerto RX1/TX1 y la conexión con el ordenador se realiza a través del puerto GB Ethernet. Por tanto, los puertos usados en el trabajo son el de la antena RX1/TX1, el del cable MIMO, el puerto GB Ethernet y la entrada de la fuente de alimentación. En la Figura 19 se puede ver la organización del panel frontal del USRP-2920.

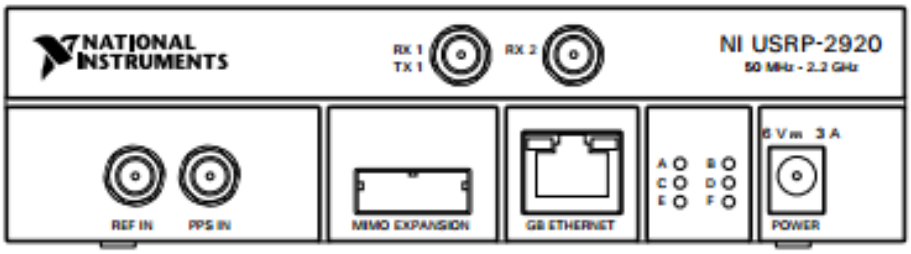

Figura 19: Panel frontal del USRP-2920 [23]

4.2. Agilent VSA 89600s

El analizador de señales Agilent VSA 89600 [24] consta de dos elementos, por un lado está la parte hardware y por otro la parte software. La parte hardware es la encargada de recibir las señales de radio y el software es el que posibilita ver como son esas señales y analizarlas. En conjunto, este analizador de señales presenta un amplio número de herramientas para analizar señales radio de más de 75 estándares y tipos de modulación.

En el trabajo realizado, el analizador de señales tan solo se ha utilizado para comprobar que durante las transmisiones se emitía en la frecuencia correcta.

Figura 20: Agilent VSA 89600 [25]

4.3. Ordenador portátil

Para la realización del TFG se ha utilizado como ordenador principal un portátil Acer TravelMate 5760 con las siguientes características:

- Procesador Intel Core i3-2310M (2x2,10 GHz / 3 Mb caché).
- 6 GB de memoria RAM DDR3 / 500 GB de disco duro (5400 rpm).
- Tarjeta gráfica nVidia GT 540M de 1 GB GDDR3.
- Sistema operativo Windows 7 Home Premium de 64 bits.

Figura 21: Ordenador portátil utilizado

Sin embargo, como se ha dicho anteriormente, fue necesario el uso de un segundo ordenador para probar el programa final. Las características del segundo ordenador son las siguientes:

- Procesador Intel Core i7 de 8 núcleos.
- 8 GB de memoria RAM / 500 GB de disco duro.
- Tarjeta gráfica integrada Intel HD Graphics 4000.
- Sistema operativo Windows 8.1 de 64 bits.

4.4. LabVIEW

LabVIEW [7] es un entorno de desarrollo creado por National Instruments diseñado principalmente para mejorar la productividad en el sector de la ingeniería. Se enfoca en la gestión de sistemas de medida y control, y ofrece una gran integración con multitud de instrumentos hardware.

La característica principal de este entorno es el uso de un lenguaje de programación gráfico, esto quiere decir que los programas no están escritos con código como es habitual, si no que todo lo que se programa se realiza utilizando pequeños bloques que realizan funciones específicas. Estos bloques, en muchos casos, simplifican gran cantidad de operaciones, ya que

hay muchos de ellos que ya están preparados para realizar las funciones habituales propias de los sistemas de medida y control. El uso de este lenguaje de programación gráfico facilita en gran medida que cualquier persona, aunque no tenga conocimientos previos de programación, pueda familiarizarse de forma rápida con la herramienta y aumentar así su productividad. También supone una ventaja a la hora de presentar al consumidor el programa, ya que es mucho más visual y la interacción con él resulta más sencilla.

En cuanto al funcionamiento del entorno de trabajo, en LabVIEW los programas se denominan VI (*Virtual Instruments*) y están divididos en dos partes que se explican a continuación:

- **Panel frontal**: es la interfaz que se le presenta al usuario, en ella se puede ver la información. En este panel se presentan dos tipos de elementos, por una parte están los controles, cuyo elige el usuario y constituyen las entradas del programa, y por otro lado están los indicadores, que representan las salidas.
- **Diagrama de bloques**: en este panel se encuentra el programa en sí, es la parte que se utiliza para definir las funciones que se aplican sobre las entradas. Estas funciones se realizan con los bloques de los que hablamos anteriormente, que se interconectan entre sí y con las entradas y salidas para formar el programa.

En las siguientes figuras (Figura 22 y Figura 23) se puede ver el panel frontal y el diagrama de bloques de un sencillo programa que realiza tres operaciones aritméticas.

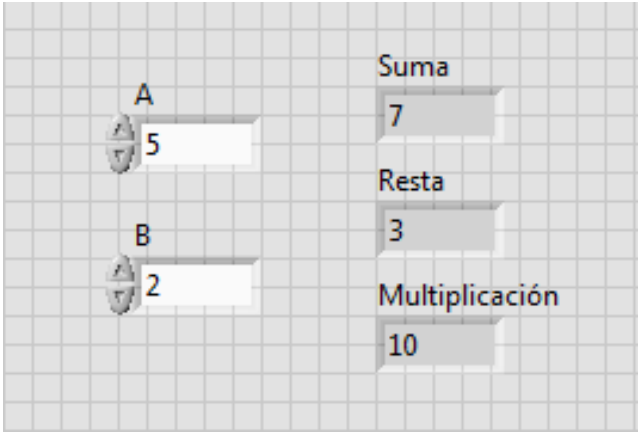

Figura 22: Panel frontal de un VI

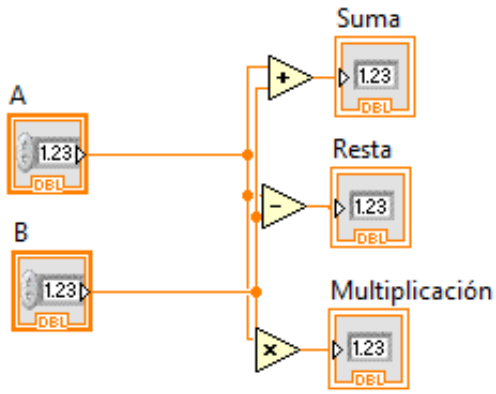

Figura 23: Diagrama de bloques de un VI

Además, en este entorno LabVIEW se incluyen funciones especiales para el uso de los transceptores NI USRP-2920 que se utilizan en el trabajo, de forma que su uso resulta muy sencillo, teniendo tan solo que configurar una serie de parámetros para que funcionen.

5. Desarrollo del proyecto

En este capítulo se explicará todo el desarrollo que se ha seguido en el TFG, desde la búsqueda de información acerca de GSM hasta el desarrollo del programa final, que simula el procedimiento "Location Update" y está divido en dos partes (estación móvil y estación base).

5.1. Planteamiento y documentación

Lo primero que se ha hecho para saber cómo empezar a desarrollar el trabajo es buscar información sobre el procedimiento que se quiere realizar. En este caso se trata de un procedimiento tan común como el "Location Update", que se produce cuando una estación móvil pasa a estar conectada a una estación base distinta porque esta le proporciona un mejor servicio. El procedimiento consiste en el intercambio de una serie de mensajes definidos entre el móvil y la nueva estación base. Este procedimiento se detalla en la Figura 24.

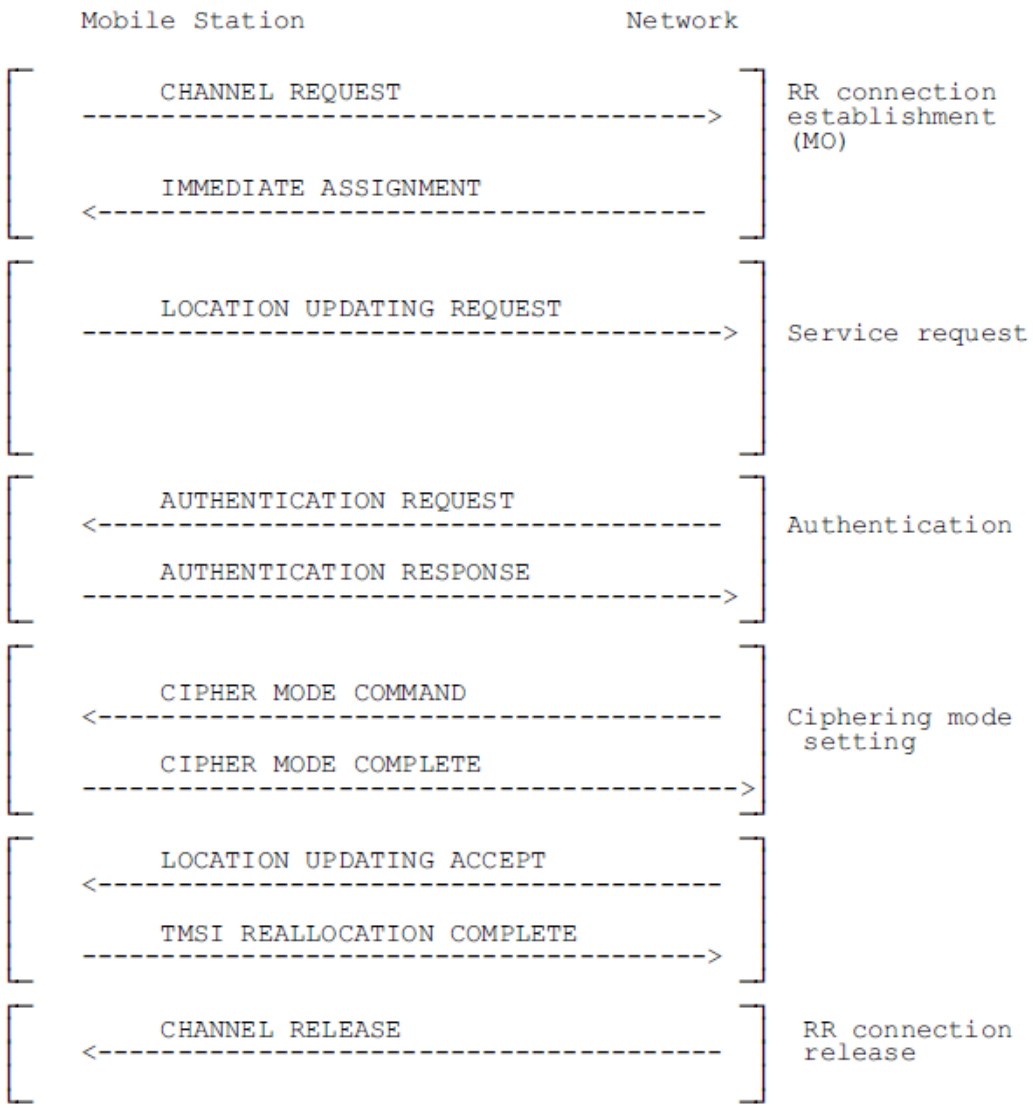

Figura 24: Procedimiento "Location Update" en GSM [26]

Una vez que tenemos claro en que consiste el procedimiento, es necesario saber cómo se forman los mensajes y qué camino siguen desde que se crean hasta que son mandados. Para obtener toda esta información se han utilizado los siguientes documentos del estándar GSM (disponibles todos desde la página del ETSI):

- GSM 03.03 - Numbering, addressing and identification [27].
- GSM 03.07 - Restoration procedures [28].
- GSM 03.08 - Organization of subscriber data [29].
- GSM 03.12 - Location registration procedures [30].
- GSM 03.20 - Security related network functions [31].
- GSM 03.22 - Functions related to Mobile Station (MS) in idle mode and group receive mode [32].
- GSM 04.08 - Mobile Radio Interface [26].
- GSM 05.01 - General Description [33].
- GSM 05.02 - Multiplexing and multiple access on the radio path [34].
- GSM 05.03 - Channel coding [35].
- GSM 05.04 - Modulation [36].
- GSM 09.02 - Mobile Application Part (MAP) specification [37].

Con todos estos documentos ya se tiene lo necesario en cuanto las características de GSM para saber cómo se implementa el procedimiento "Location Update".

En lo que respecta al uso del software y el hardware utilizado, no es necesaria una gran base previa para comprender como utilizarlo. Con ver algunos tutoriales disponibles en Internet [38] resulta suficiente para ver cómo funciona el entorno LabVIEW, aunque para la realización de algún paso sí que haya sido necesaria la búsqueda de información más específica. Por otro lado, el uso de los transceptores USRP-2920 es bastante sencillo y no requiere de ninguna configuración compleja, esto se debe principalmente a los bloques que ya vienen implementados en LabVIEW para el manejo de los mismos.

A modo de resumen, y como introducción a lo que se realiza en el siguiente apartado, se puede describir el proceso que sigue cada mensaje como una serie de pasos:

1. Creación del mensaje, rellenando el mismo con todos los campos que se indican en el estándar según cada caso.
2. Codificación del mensaje creado, usando los algoritmos correspondientes según el canal lógico que se use como portador del mismo.
3. Creación de las ráfagas.
4. Modulación de las ráfagas.
5. Inclusión de las ráfagas moduladas en un slot.
6. Creación de las tramas con la unión de ocho slots.
7. Envío de las tramas a través del USRP-2920.
8. Recepción de la trama gracias a otro USRP-2920.
9. A partir de la trama recibida se obtiene el mensaje comparando con un patrón fijo conocido del mismo.

10. Decodificación del mensaje y obtención de los datos del mismo.

Una vez completados todos estos pasos ya tendríamos el mensaje original en el receptor, habiendo completado el envío. Este proceso se debe repetir una vez por cada mensaje que se envía en la comunicación, y hasta que no se envíen y reciban todos no se puede dar como correcto el procedimiento.

No obstante, todo el proceso que se sigue no es exactamente igual que en GSM, ya que hay algunos pasos (como la organización de las tramas en multitramas o la sincronización entre la estación base y el móvil) que no se realizan. Esto es debido a que para el ejemplo que se quiere ilustrar con este trabajo no es necesario realizarlo, o puede complicar mucho el desarrollo del mismo. Además, como ya se comentó en el capítulo 1, estos procesos pueden ser el contenido de otros trabajos que se realicen en el futuro.

5.2. Diseño de los módulos del programa

Para la implementación del procedimiento, se ha dividido el programa en varios bloques que realizan las diversas tareas que se han resumido anteriormente.

5.2.1. Creación de los mensajes

Cómo se pudo ver en la Figura 24, son varios los mensajes implicados en el procedimiento. Todos estos mensajes están definidos en el estándar de GSM [26] y se explica que contiene cada uno de los campos que los forman. En este apartado se va a ver cuáles son esos campos y que información llevan en cada caso, así como la creación de estos mensajes dentro de un VI de LabVIEW.

5.2.1.1. Channel Request

El mensaje "Channel Request" es el que usa la estación móvil en GSM para pedir a la red los recursos necesarios para iniciar la comunicación. Como se expuso en el capítulo 3, donde se explicaba el funcionamiento de GSM, estas peticiones se realizan a través de RACH, y se envían a través de una ráfaga de acceso.

El mensaje está formado por 8 bits organizados según se indica en la Figura 25.

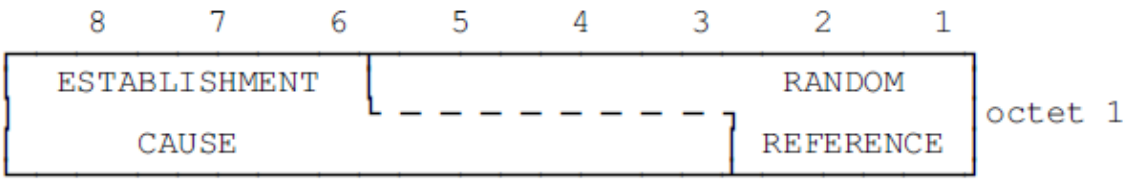

Figura 25: Contenido del "Channel Request" [26]

El campo "`Establishment Cause`" indica la causa de la petición para establecer la conexión y tiene un tamaño variable de 3 a 6 bits. En el caso del "Location Update", estos bits

pueden ser "**000**" o "**0000**" dependiendo de si la red soporta el uso de canales TCH/HS o no. En este trabajo se da por hecho que la red sí soporta estos canales y se usa "**0000**".

Por otro lado, el campo "Random Reference" no presenta un contenido definido y tiene una longitud variable de 2 a 5 bits. Por esta razón, en el trabajo se usan 4 bits cualesquiera.

5.2.1.2. Immediate Assigment

El mensaje "Immediate Assigment" es enviado desde la red a la estación móvil para asignarle un canal lógico y realizar la configuración del mismo. El canal usado para enviar este mensaje es el AGCH y los campos de los que consta se exponen en la Tabla 2.

Elemento de información	Tipo	Longitud (en octetos)
L2 Pseudo Length	L2 Pseudo Length	1
RR Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Immediate Assigment Message Type	Message Type	1
Page Mode	Page Mode	½
Spare Half Octet	Spare Half Octet	½
Channel Description	Channel Description	3
Request Reference	Request Reference	3
Timing Advance	Timing Advance	1
Mobile Allocation	Mobile Allocation	1-9
Starting Time	Starting Time	3
IA Rest Octets (frequency, parameters, before time)	IA Rest Octets	0-11

Tabla 2: Campos del "Immediate Assigment"

Como varios de los parámetros que forman el mensaje tienen valores que pueden cambiar según las circunstancias, solo se expondrán los campos que se deben establecer explícitamente porque tienen un valor fijo. Los valores que no se exponen se completarán con bits de relleno, aunque en el código será posible modificarlos fácilmente.

- **"Protocol Discriminator"**: como es un mensaje relativo al control de los recursos radio, el contenido de este campo es "**0110**".

- **"Skip Indicator"**: cualquier mensaje que en este campo contenga otra cosa que no sean cuatro ceros se ignorará, por tanto el contenido del mismo es "**0000**".
- **"Message Type"**: indica que tipo de mensaje se está enviando, en el caso de un "Immediate Assigment" el contenido de este campo es "**00111111**".

5.2.1.3. Location Updating Request

Este mensaje es uno de los más importantes en el procedimiento, ya que es el que manda la estación móvil a la red para pedir la actualización de su localización. Este mensaje se envía a través del SDCCH y consta de los campos que se indican en la Tabla 3.

Elemento de información	Tipo	Longitud (en octetos)
Mobility Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Location Updating Request Message Type	Message Type	1
Location Updating Type	Location Updating Type	½
Ciphering Key Sequence Number	Ciphering Key Sequence Number	½
Location Area Identification	Location Area Identification	5
Mobile Station Classmark 1	Mobile Station Classmark 1	1
Mobile Identity	Mobile Identity	2-9

Tabla 3: Campos del "Location Updating Request"

En este caso también se realizará una explicación de los campos que se ponen explícitamente, y se completarán los restantes con bits de relleno.

- **"Protocol Discriminator"**: como se trata de un mensaje de gestión de movilidad, este campo contiene los bits "**0101**".
- **"Skip Indicator"**: Como ya se expuso, este campo ha de ser "**0000**".
- **"Message Type"**: para el "Location Updating Request" los bits de este campo son "**0X001000**", donde la X indica el tipo de enlace en el que se envía el mensaje (ascendente o descendente). En este caso se trata del enlace ascendente y la X debe ser "**1**".
- **"Location Updating Type"**: este campo está compuesto de dos bits que indican el tipo de actualización de la localización (los dos primeros bits), otro bit a "**0**", y el último bit que indica si existe una petición pendiente. El primer campo se debe rellenar en el caso de este trabajo con "**00**", ya que se trata de un "Normal Location Updating", y el último bit también ha de ser "**0**" porque no existe ninguna petición

pendiente. Por tanto, el campo se rellena con "**0000**". En la Figura 26 podemos ver cómo está organizado.

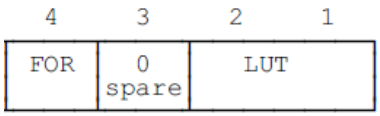

Figura 26: Estructura del "Location Updating Type" [26]

- **"Location Area Identification" (LAI)**: este campo es de gran importancia porque en él se indica el área en la que se encuentra el móvil. El contenido de este campo depende del MCC (*Mobile Country Code*), del MNC (*Mobile Network Code*)[3] y del LAC (*Location Area Code*), por tanto varía en función de la localización. El contenido de este campo se organiza como se indica en la Figura 27.

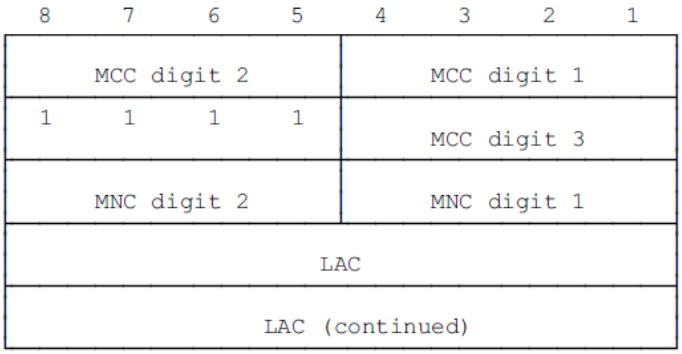

Figura 27: Estructura del "Location Area Identification" [26]

5.2.1.4. Authentication Request

Este mensaje se envía desde la red a la estación móvil para comenzar la autentificación de la identidad del móvil. Se envía por el canal SDCCH y consta de los campos que aparecen en la Tabla 4.

Elemento de información	Tipo	Longitud (en octetos)
Mobility Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Authentication Request Message Type	Message Type	1
Ciphering Key Sequence Number	Ciphering Key Sequence Number	½
Spare Half Octet	Spare Half Octet	½
Authentication Parameter RAND	Authentication Parameter RAND	16

Tabla 4: Campos del "Authentication Request"

[3] Estos códigos se pueden consultar en Internet [39]

En este caso se indicará el contenido de los tres primeros parámetros, ya que los otros tres hacen referencia a parámetros de la autenticación que no son de especial interés en este trabajo.

- **"Protocol Discriminator"**: esta vez también se trata un mensaje para el control de la movilidad y, por tanto, su valor es "**0101**"
- **"Skip Indicator"**: ya hemos visto que ha de ser "**0000**".
- **"Message Type"**: en este caso es "**0X010010**", siendo esta vez la X igual a "**1**" porque el mensaje se envía desde la red a la estación móvil.

5.2.1.5. Authentication Response

Este mensaje se lo manda el móvil a la red como respuesta al "Authentication Request", en él se contesta a la petición de autenticación a través del parámetro SRES, que es una respuesta firmada del parámetro RAND. El envío se realiza a través del SDCCH y el mensaje está formado por los campos que se indican en la Tabla 5.

Elemento de información	Tipo	Longitud (en octetos)
Mobility Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Authentication Response Message Type	Message Type	1
Authentication Parameter SRES	Authentication Parameter SRES	4

Tabla 5: Campos del "Authentication Response"

Al igual que pasaba en el mensaje "Authentication Request", los campos que podríamos rellenar son los tres primeros, dado que el cuarto es la respuesta firmada que se comentó antes y depende del mensaje anterior.

- **"Protocol Discriminator"**: al igual que antes, su valor es "**0000**".
- **"Skip Indicator"**: como se ha visto, su valor es "**0000**".
- **"Message Type"**: en este caso es "**0X010100**", con la X igual a "**1**" por ser enviado desde el móvil a la red.

5.2.1.6. Cipher Mode Command

Este mensaje se envía desde la red a la estación móvil para indicar a este que la red ha empezado a descifrar y que el cifrado y descifrado debe comenzar por parte del móvil, o para indicar que el cifrado no será implementado. El envío se realiza a través del SDCCH y la composición del mensaje se describe en la Tabla 6.

Como ocurría con los mensajes referentes a la autenticación, para este trabajo no es de gran interés el proceso de cifrado en la red, ya que constituye un proceso a parte del "Location Update".

Elemento de información	Tipo	Longitud (en octetos)
RR Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Cipher Mode Command Message Type	Message Type	1
Ciphering Mode Setting	Ciphering Mode Setting	½
Cipher Response	Cipher Response	½

Tabla 6: Campos del "Cipher Mode Command"

En este caso, como con los anteriores, nos centraremos en los campos fijos que podemos rellenar, dejando aparte los que dependen de parámetros de cifrado.

- **"Protocol Discriminator"**: en este caso es un mensaje relativo a la gestión de los recursos radio, por lo que su valor es "**0110**".
- **"Skip Indicator"**: como siempre, su valor es "**0000**".
- **"Message Type"**: en este caso es "**00110101**".

5.2.1.7. Cipher Mode Complete

Se envía desde el móvil a la red para indicar que este ha comenzado el cifrado y descifrado. El canal usado es el SDCCH y los campos del mensaje se indican en la Tabla 7.

Elemento de información	Tipo	Longitud (en octetos)
RR Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Cipher Mode Complete Message Type	Message Type	1
Mobile Equipment Identity	Mobile Identity	3-11

Tabla 7: Campos del "Cipher Mode Complete"

Como antes, veremos el contenido de los tres primeros campos.

- **"Protocol Discriminator"**: como en el caso anterior, se trata de un mensaje relativo a la gestión de los recursos radio y su valor es "**0110**".
- **"Skip Indicator"**: como siempre, su valor es "**0000**".
- **"Message Type"**: en este caso los cinco primeros bits son iguales que los del caso anterior, ya que se trata de un mensaje relativo al cifrado. El cambio se da en los tres últimos bits del campo, siendo el contenido completo "**00110010**".

5.2.1.8. Location Updating Accept

Este mensaje se envía desde la red a la estación móvil para indicar que la actualización de la localización se ha completado. El canal utilizado es el SDCCH y los campos del mensaje se pueden ver la Tabla 8.

Elemento de información	Tipo	Longitud (en octetos)
Mobility Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Location Updating Accept Message Type	Message Type	1
Location Area Identification	Location Area Identification	5
Mobile Identity	Mobile Identity	3-10
Follow On Proceed	Follow On Proceed	1

Tabla 8: Campos del "Location Updating Accept"

En este caso, la mayoría de los campos del mensaje que definimos de forma explícita son iguales a los del "Location Updating Request", tan solo cambiaría el "Message Type.

- **"Protocol Discriminator"**: al ser de gestión de movilidad su valor es "**0101**".
- **"Skip Indicator"**: su contenido es "**0000**".
- **"Message Type"**: en este caso su valor es "**0X000010**", siendo X igual a "**0**" por ser un mensaje enviado desde la red al móvil.
- **"Location Area Identification"**: ya se vio al explicar el "Location Updating Request" que este campo depende de la zona en la que se encuentre la celda. La estructura de este campo se expuso en la Figura 27.

5.2.1.9. TMSI Reallocation Complete

Este mensaje se envía desde el móvil a la red para indicar que se ha producido la reasignación del TMSI, cambiando el que tenía en su antigua celda por el de la nueva. Este mensaje se envía a través del SDCCH y su estructura se indica en la Tabla 9.

Elemento de información	Tipo	Longitud (en octetos)
Mobility Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
TMSI Reallocation Message Type	Message Type	1

Tabla 9: Campos del "TMSI Reallocation Complete"

Como se ve, este mensaje solo consta de los tres campos que hemos visto en todos los demás mensaje.

- **"Protocol Discriminator"**: como se trata de un mensaje de gestión de movilidad, este campo contiene los bits "**0101**".
- **"Skip Indicator"**: como siempre, su valor es "**0000**".
- **"Message Type"**: en este caso es "**0X011011**", siendo la X igual a "**1**" porque el mensaje se envía desde la estación móvil a la red.

5.2.1.10. Channel Release

Este mensaje se envía desde la red al móvil para iniciar la desactivación del canal dedicado que se ha usado en la comunicación. Se envía a través del SDCCH y su contenido se indica en la Tabla 10.

Elemento de información	Tipo	Longitud (en octetos)
RR Management Protocol Discriminator	Protocol Discriminator	½
Skip Indicator	Skip Indicator	½
Immediate Assigment Message Type	Message Type	1
RR Cause	RR Cause	1
BA Range	BA Range	6-?
Group Channel Description	Group Channel Description	4-13
Group Cipher Key Number	Group Cipher Key Number	1 ½

Tabla 10: Campos del "Channel Release"

Los campos que veremos son lo que tienen un contenido fijo en este caso, dejando aparte los que dependen de las circunstancias concretas.

- **"Protocol Discriminator"**: en este caso es un mensaje relativo a la gestión de los recursos radio, por lo que su valor es "**0110**".
- **"Skip Indicator"**: como siempre, su valor es "**0000**".
- **"Message Type"**: en el caso de este mensaje su valor es "**00001101**".
- **"RR Cause"**: este campo indica la razón por la que se ha mandado el mensaje, en el caso de un evento normal como este su valor es "**00000000**".

5.2.1.11. VI – Mensajes

Para implementar los mensajes dentro de LabVIEW se ha creado un VI específico en el que se indican todos los campos. Este VI se ha denominado "Mensajes SDCCH.vi" porque en él se implementan los mensajes que se usan en el SDCCH. Los mensajes que no usan el SDCCH se

crean dentro del VI encargado de la codificación en cada caso (en el RACH y el AGCH) como se verá en el apartado de la codificación.

Como se muestra en la Figura 28 donde aparece cómo se forma un "Location Updating Request", en el VI se indican todos los campos que forman el mensaje, siendo posible cambiarlos fácilmente. En este bloque están implementados todos los mensajes que se han visto a excepción del "Channel Request" y el "Immediate Assigment", que como se ha dicho antes se crean en otros VI.

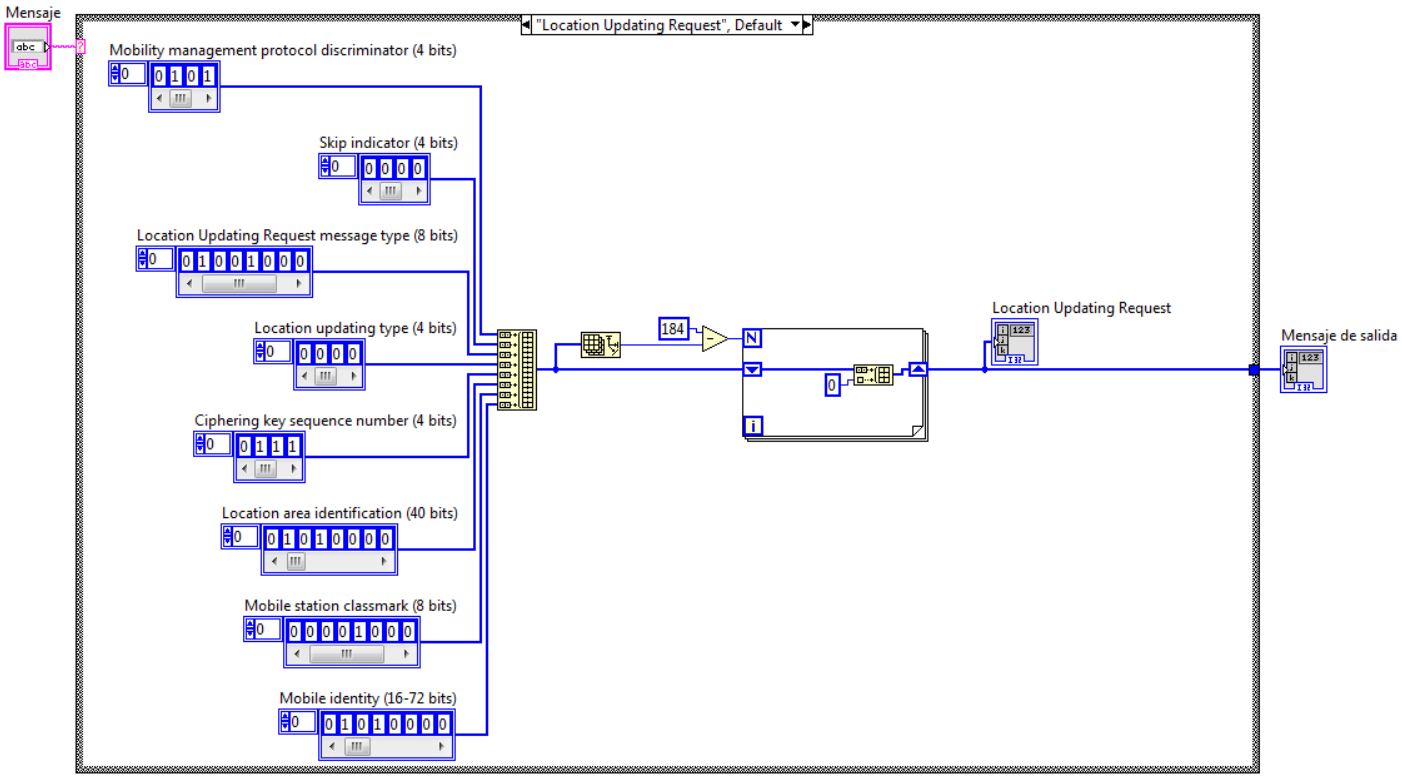

Figura 28: "Mensajes SDCCH.vi"

El bloque solo cuenta con un String como entrada ("Mensaje"), que sirve como selector en la estructura Case para elegir qué mensaje se quiere obtener. La salida es un Array de bits ("Mensaje de salida") con el mensaje elegido.

Lo que se hace para obtener el mensaje en todos los casos es unir los campos que lo componen y rellenar con ceros (en caso de ser necesario) para completar los 184 bits que necesita el codificador del SDCCH.

5.2.2. Codificación de los mensajes

Como se vio en el capítulo 3, los mensajes pasan por un proceso de codificación antes de formar una ráfaga, este proceso se detalla en el estándar de GSM [35]. En este apartado se explicará cómo es esa codificación para los canales que se han utilizado en el trabajo, y cómo se ha implementado en LabVIEW.

5.2.2.1. RACH

El RACH es el canal usado para mandar el primer mensaje del procedimiento ("Channel Request"). Este mensaje consta de 8 bits que, tras el proceso de codificación, pasan a ser 36. Este proceso consta principalmente de cuatro pasos:

- Obtención de 6 bits de paridad (p(k)) a partir de los 8 bits de información (d(k)) de la siguiente manera (todas las operaciones se realizan en módulo 2):
  $d(0)D^{13} + ... + d(7)D^6 + p(0)D^5 + ... + p(5)$, al dividirlo entre $D^6 + D^5 + D^3 + D^2 + D + 1$ da como resultado el resto $D^5 + D^4 + D^3 + D^2 + D + 1$.
- A continuación, se realiza una suma en módulo 2 entre los bits de paridad obtenidos y los 6 bits del BSIC(*Base Station Identity Code*) (b(k)) para obtener lo que se conoce como los bits de color (C(k)).
- A los 8 bits de información se les agregan estos 6 bits de color y otros 4 bits de cola para dar como resultado 16 bits (u(k)).
- Por último, se realiza una codificación convolucional de tasa ½ para dar los 36 bits de salida (e(k)). La codificación convolucional viene determinada por la siguiente fórmula:
  e(2k) = u(k) + u(k-3) + u(k-4)
  e(2k+1) = u(k) + u(k-1) + u(k-3) + u(k-4) para k = 0,1,...,17 ; u(k) = 0 para k < 0

El VI encargado de realizar la codificación del RACH se ha denominado "RACH.vi" y se muestra en la Figura 29.

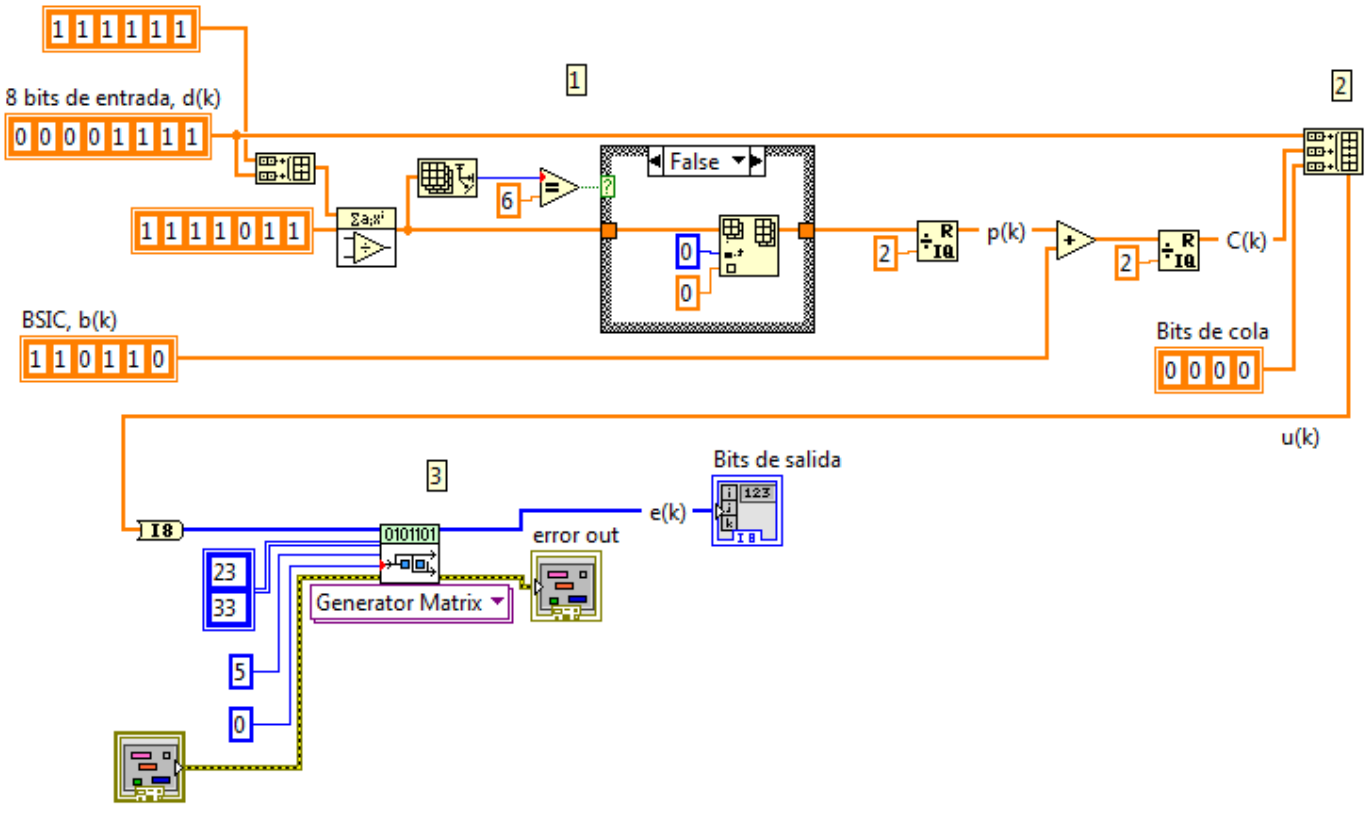

Figura 29: "RACH.vi"

Este bloque no tiene ninguna entrada efectiva ya el mensaje a codificar se especifica dentro del mismo bloque ("8 bits de entrada, d(k)"), y la única salida son los 36 bits del mensaje codificado ("Bits de salida").

Todo el proceso que se ha explicado antes está señalizado en el bloque. En la parte 1 se calculan los bits de paridad y se les suma el BSIC (en este caso se usan unos bits cualquiera), en la parte 2 se añade esta suma junto con los bits de cola al mensaje original, y en la parte 3 se realiza la codificación convolucional.

5.2.2.2. AGCH

El AGCH se usa para mandar el segundo mensaje del procedimiento ("Immediate Assigment"). Este mensaje consta de 184 bits que, tras el proceso de codificación, pasan a ser 456. Este proceso se puede dividir en 4 procesos:

- Lo primero que se hace es calcular los bits de paridad (p(k)) a partir de un código FIRE, este código obtiene 40 bits a partir de los 184 bits de información (d(k)). La obtención de los bits se realiza de la siguiente manera (todas las operaciones son en módulo 2):
  $d(0)D^{223} + d(1)D^{222}+...+d(183)D^{40} + p(1)D^{38}+...+p(38)D + p(39)$ al dividirlo entre $(D^{23} + 1)*(D^{17} + D^3 + 1)$ da como resultado el resto $1 + D + D^2 +...+ D^{39}$.
- A los 184 bits de información se le añaden los 40 bits de paridad más 4 bits de cola, lo que da como resultado 228 bits (u(k)).
- Estos 228 bits pasan por un codificador convolucional de tasa ½ para obtener 456 bits (c(k)). Esta codificación convolucional viene dada por la fórmula:
  c(2k) = u(k) + u(k-3) + u(k-4)
  c(2k+1) = u(k) + u(k-1) + u(k-3) + u(k-4) para k = 0,1,...,227 ; u(k) = 0 para k < 0
- Por último se realiza un entrelazado que divide los 456 bits en 4 grupos de 114 bits para que puedan ser enviados en una Normal Burst. Este proceso se realiza con la siguiente fórmula:
  i(B,j) = c(k) para k = 0,1,...,455
  B = k mod 4
  j = 2((49k) mod 57) + ((k mod 8) div 4)
  Siendo i(0,j) el primer grupo, i(1,j) el segundo, i(2,j) el tercero e i(3,j) el cuarto.

Además existe un último paso que explica cómo se realiza el mapeo de estos grupos dentro de la ráfaga en la que irán, ya que el contenido efectivo de una Normal Burst son 116 bits y, por tanto, es necesario añadir 2 bits a los 114 que ya se tienen. Este mapeo está definido de la siguiente forma:
e(B,j) = i(B,j) y e(B,59+j) = i(B,57+j) para j = 0,1,...,56 y e(B,57) = e(B,58) = "1"

No obstante, este paso se realizará al crear las ráfagas por lo que en este bloque no se tiene en cuenta.

El VI encargado de realizar la codificación del AGCH se ha denominado "AGCH.vi", y se presenta en las Figura 30 y 31 (la figura 31 es una continuación de la 30, se presenta así para una mejor visualización).

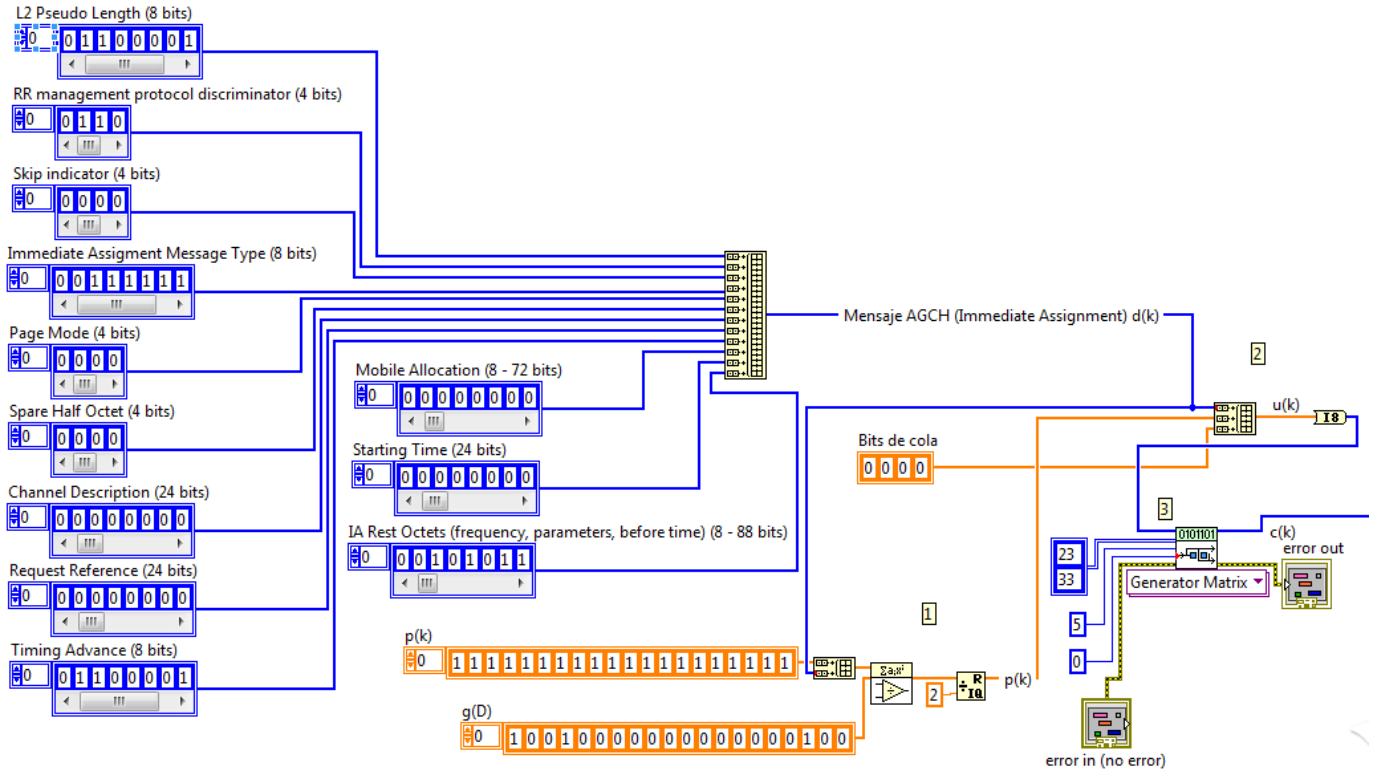

Figura 30: "AGCH" parte 1

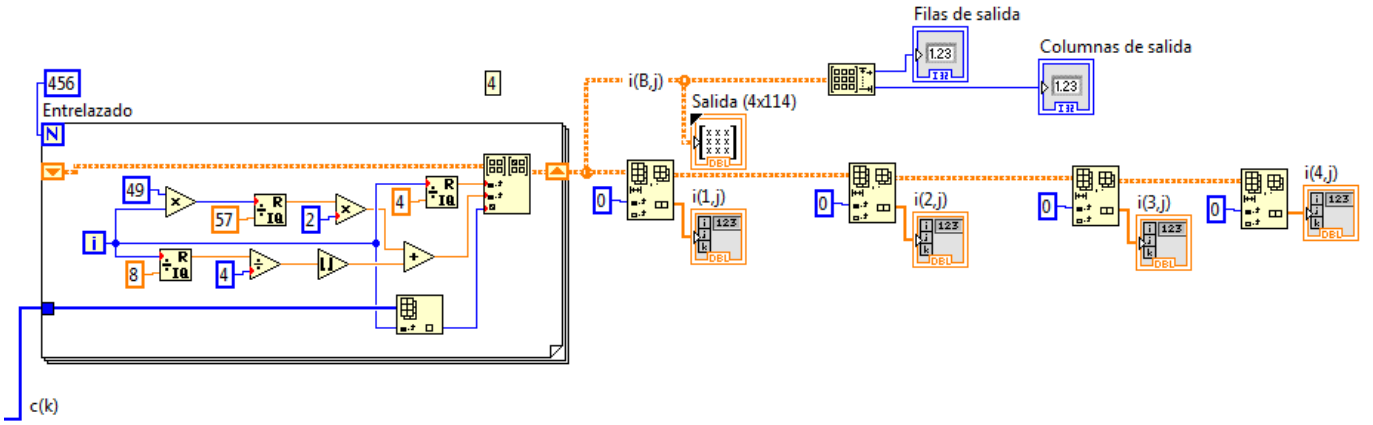

Figura 31: "AGCH" parte 2

Como ocurría con el RACH, este bloque no tiene ninguna entrada efectiva, dado que los 148 bits del mensaje a codificar están incluidos dentro del propio bloque. El mensaje consta de todos los campos que se vieron antes, los cuales pueden cambiarse fácilmente si fuera necesario. Por otra parte consta de 4 salidas correspondientes a los 4 grupos de 114 bits que se extraen de la matriz de 4x114 que sale del entrelazado.

Los pasos que se han explicado están indicados en el bloque. La parte 1 corresponde a la obtención de los 40 bits de paridad, en la parte 2 se unen estos bits de paridad junto con los de cola a los 148 bits de información, en la parte 3 se realiza la codificación convolucional y, por último, en la parte 4 se realiza el entrelazado y la separación de los grupos de 114 bits.

5.2.2.3. SDCCH

El SDCCH se usa para mandar todos los mensajes restantes del procedimiento. Todo el proceso de codificación es exactamente igual que en el AGCH, por lo que no es necesario explicarlo en este apartado.

El VI encargado de realizar la codificación del SDCCH se ha denominado "SDCCH coding.vi" y es igual que el "AGCH.vi", con la única excepción de que este sí consta de una entrada por la que se introduce el mensaje de 148 bits a codificar.

5.2.3. Creación de las ráfagas

Tras la codificación, los mensajes se insertan dentro de ráfagas antes de ser modulados e incluidos en una trama. En el caso de este trabajo solo es necesario el desarrollo de dos tipos de ráfagas, la "Access Burst" y la "Normal Burst".

Ambos tipos de ráfagas ya se expusieron en el capítulo 3, donde se puede ver su estructura gracias a las Figuras 10 y 14.

5.2.3.1. Access Burst

La composición de la ráfaga de acceso se detalla en la Tabla 11.

Numero de bit (BN)	Longitud del campo	Contenido del campo
0-7	8	Extended Tail Bits
8-48	41	Synch. Sequence Bits
49-84	36	Encrypted Bits (e0 .. e35)
85-87	3	Tail Bits
88-156	68,25	Extended Guard Period (bits)

Tabla 11: Contenido de la "Access Burst"

Donde:

- Los "Extended Tail Bits" están definidos como bits de modulación con el valor "00111010".
- Los "Synch. Sequence Bits" están definidos como bits de modulación con el valor "0100101101111111100110011010101000111100O".
- Los "Encrypted Bits" son los bits codificados que se quieren enviar.
- Los "Tail Bits" están definidos como bits de modulación con el valor "000".
- Los "Extended Guard Period" no son bits en sí, si no que representan el tiempo equivalente a los bits que se indican. Este tiempo es necesario porque los móviles requieren que la transmisión sea atenuada un tiempo entra ráfagas.

5.2.3.2. Normal Burst

La composición de la ráfaga normal se detalla en la Tabla 12.

Numero de bit (BN)	Longitud del campo	Contenido del campo
0-2	2	Tail Bits
3-60	58	Encrypted Bits (e0 .. e57)
61-86	26	Training Sequence Bits
87-144	58	Encrypted Bits (e58 .. e115)
145-147	3	Tail Bits
148-159	8,25	Guard Period (bits)

Tabla 12: Contenido de la "Normal Burst"

Donde:

- Los "Tail Bits" están definidos como bits de modulación con el valor "000".
- Los "Encrypted Bits" son los 114 bits de información que se dividen en dos y se les añade un bit a cada parte (como se indicó al explicar el mapeo en la ráfaga dentro de la codificación) para ocupar los dos campos de 58 bits disponibles.
- Los "Training Sequence Bits" son 26 bits que están fijados por la estación base. Estos bits dependen del TSC (*Training Sequence Code*), que debe ser igual al BCC (*Base Station Color Code*), existiendo 8 combinaciones distintas de bits.
- Los "Guard Period Bits", como se explicó anteriormente, representan el tiempo equivalente a los bits que indican.

5.2.3.3. VI – Ráfagas

El VI encargado de la creación de las ráfagas se ha denominado "Burst.vi" y se tiene la opción de crear "Normal Burst" y "Access Burst" como se indica en las Figuras 32 y 33.

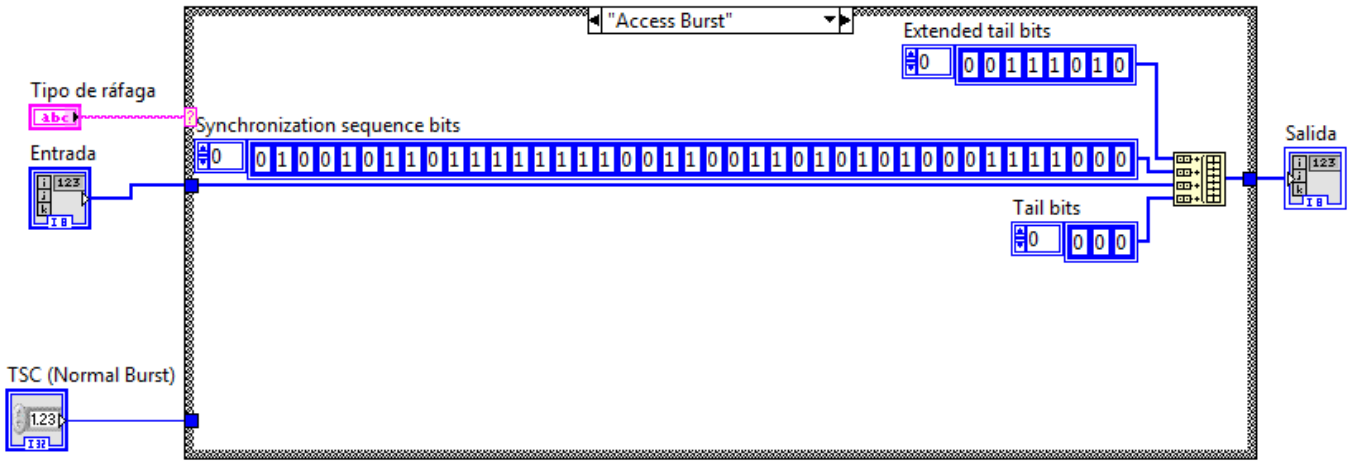

Figura 32: "Burst.vi" (Access Burst)

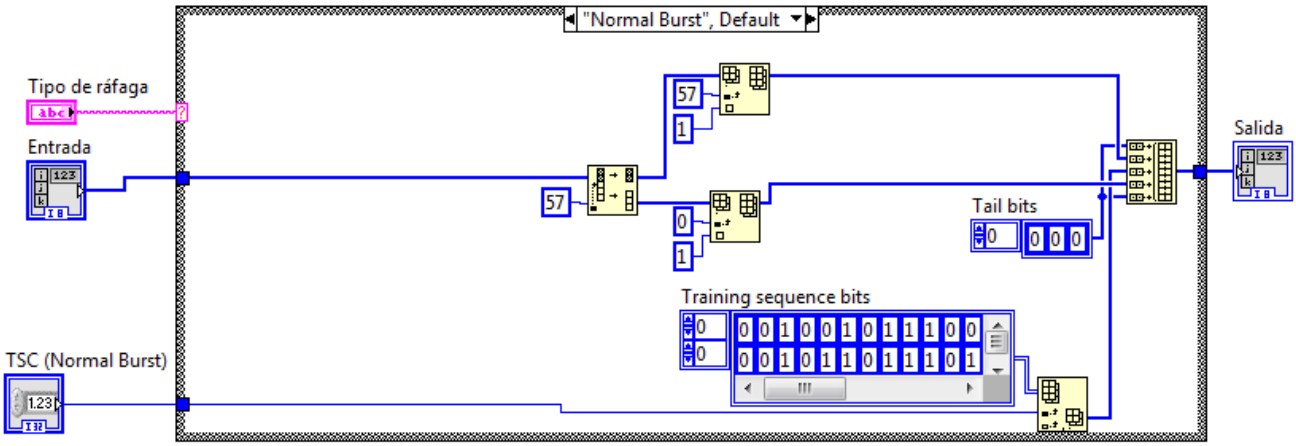

Figura 33: "Burst.vi" (Normal Burst)

Este bloque consta de tres entradas que se explican a continuación:

- "Tipo de ráfaga": esta entrada es un String que indica a la estructura Case si la ráfaga a crear es una "Access Burst" o una "Normal Burst".
- "Entrada": este es el mensaje que se quiere introducir en la ráfaga y que, en el caso de la ráfaga normal, está compuesto de 114 bits que corresponden a una de las cuatro partes en las que se divide el mensaje en la codificación.
- "TSC (Normal Burst)": esta entrada indica cual es la TSC (0-7) que se ha de usar en caso de que se elija la "Normal Burst".

En cuanto a la salida "Salida" es única y devuelve un Array de bits con la ráfaga creada.

Este VI crea las ráfagas como se ha indicado en los apartados anteriores, a excepción del periodo de guarda, que se incluirá más adelante en la creación de las tramas.

5.2.4. Modulación

Como se explicó en el capítulo 3, en GSM se usa una modulación GMSK, que es una modulación MSK con un filtro gaussiano. El VI encargado de realizar la modulación se ha denominado "Modulador.vi" y se muestra en la Figura 34.

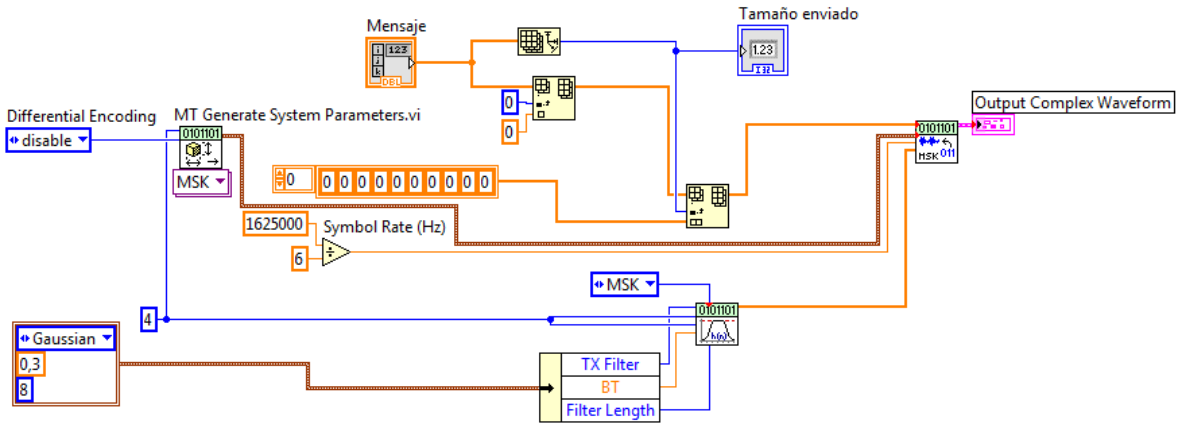

Figura 34: "Modulador.vi"

En este bloque se utilizan las herramientas que ofrece LabVIEW para modular señales. De forma concreta se usa el módulo que realiza una modulación MSK y se le añaden los parámetros del filtro gaussiano usado en GSM. También se realiza alguna pequeña modificación como añadir el Symbol Rate teórico de GSM.

La única entrada que tiene este bloque es "Mensaje", que contiene el Array de bits que se quiere modular. En cuanto a la salida, también es única y se trata de "Output Complex Waveform", que devuelve la forma de onda resultante tras la modulación.

5.2.5. Creación de tramas

Como ya se vio, una trama está formada por 8 slots que, a su vez, contienen una ráfaga cada uno. Para la creación de las tramas se utiliza el VI "Tramas.vi" que se puede ver en la Figura 35.

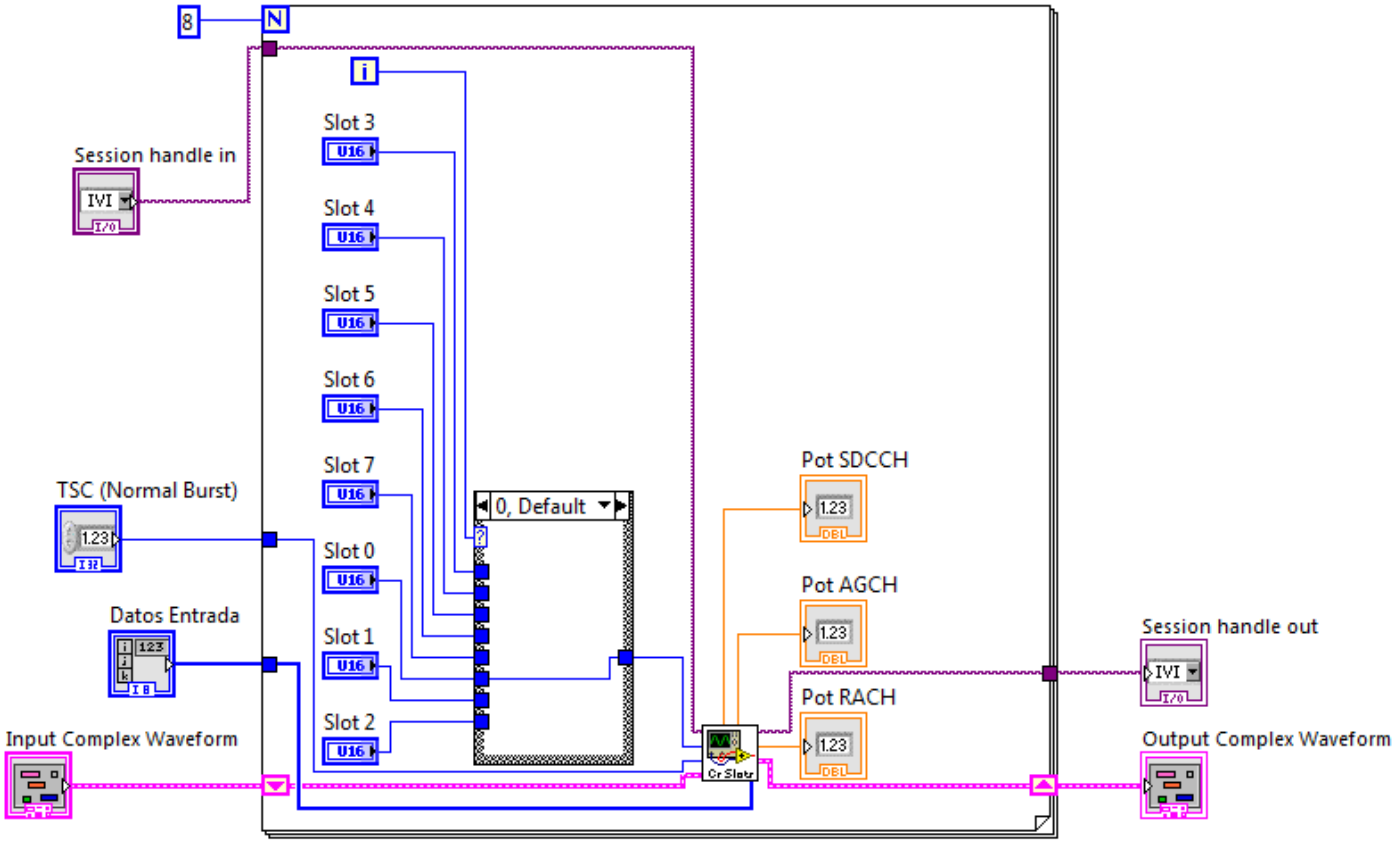

Figura 35: "Trama.vi"

Este bloque recibe una forma de onda (generalmente vacía) para ir añadiendo la forma de onda de cada slot a la trama. Esto lo consigue gracias a un bucle For que se repite 8 veces. Realmente este VI tan solo es una herramienta para completar la trama que llevará la información de un slot, dejándose el resto vacíos. El núcleo de este bloque es otro VI denominado "Crear Slot.vi", que es el encargado de crear una ráfaga, modularla, añadir el tiempo de guarda y devolver el resultado como la forma de onda correspondiente a un slot. Por tanto las entradas y salidas de "Tramas.vi" son las mismas que las de "Crear Slot.vi".

Este VI ("Crear Slot.vi") se muestra en las Figuras 36, 37, 38 y 39.

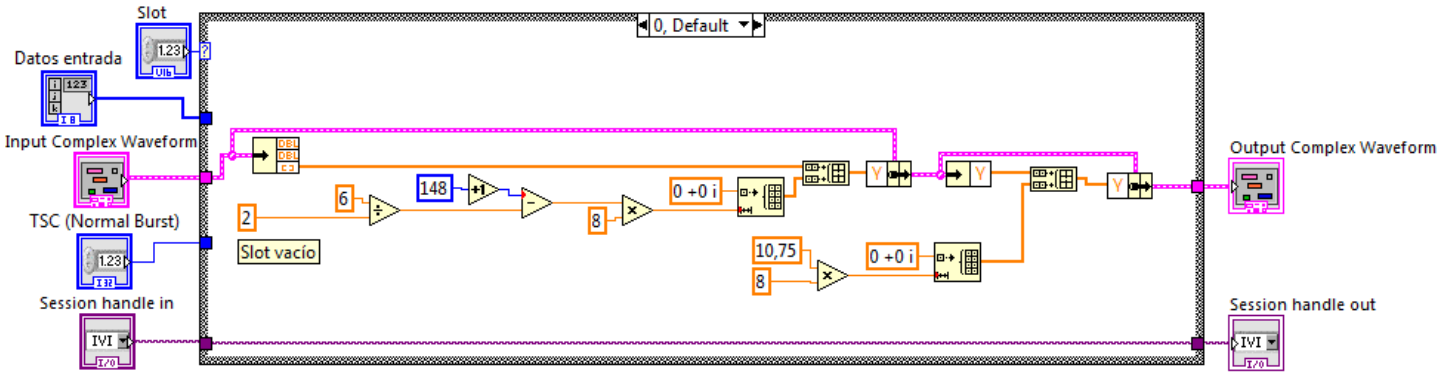

Figura 36: "Crear Slot" (vacío)

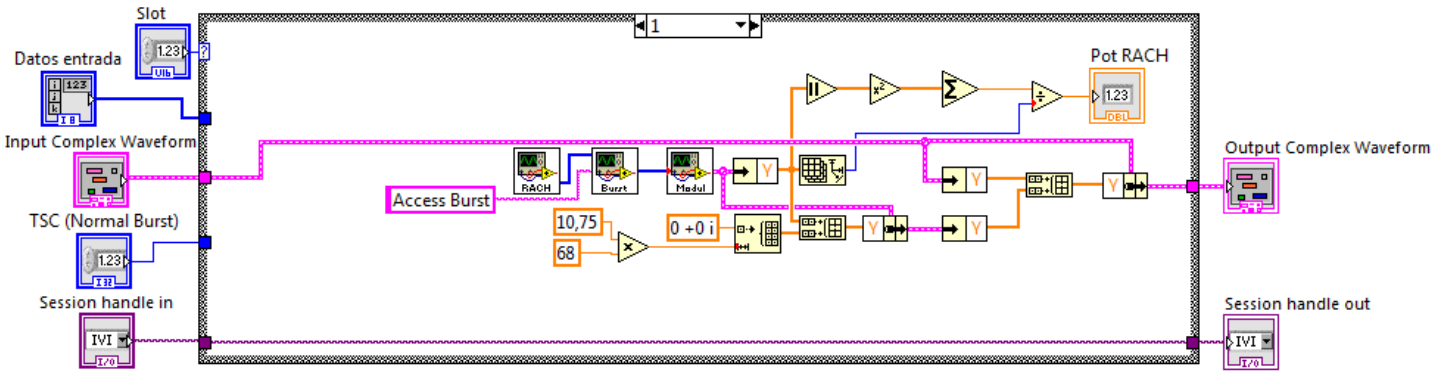

Figura 37: "Crear Slot" (RACH)

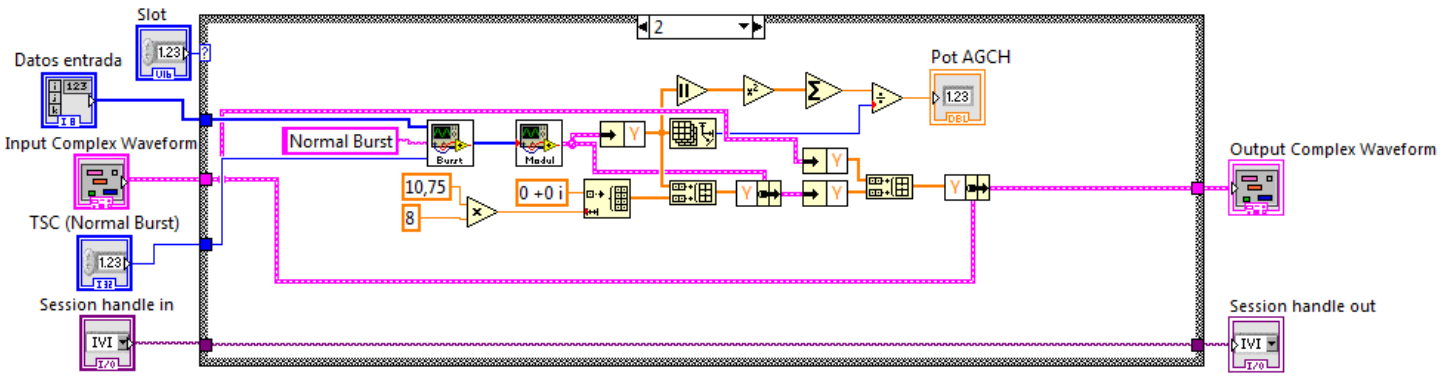

Figura 38: "Crear Slot" (AGCH)

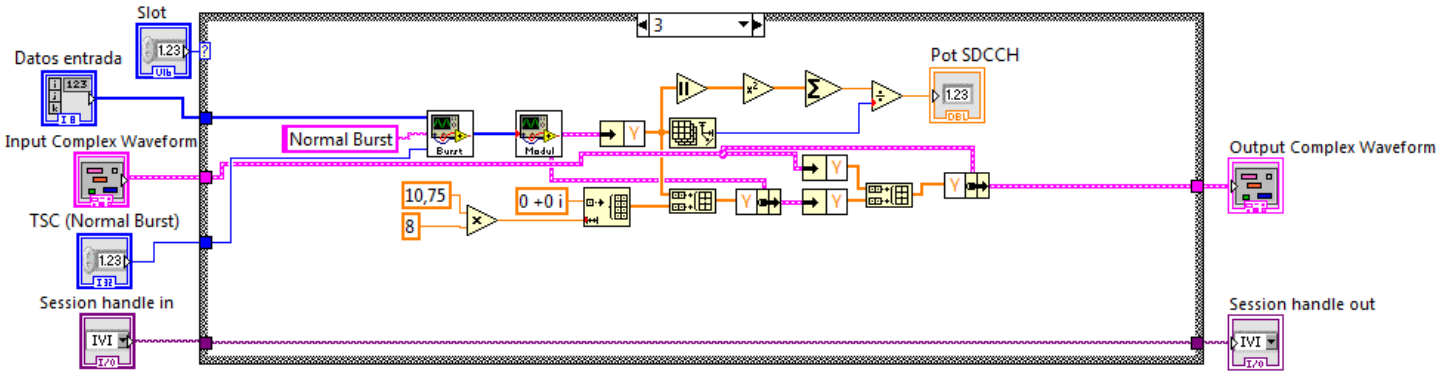

Figura 39: "Crear Slot" (SDCCH)

Las entradas de este bloque son las siguientes:

- "Slot": indica el tipo de canal lógico que se ha de crear gestionando la estructura Case. Los posibles casos de esta estructura son:
  - 0: Crea un slot vacío.
  - 1: Crea un slot con el RACH.
  - 2: Crea un slot con el AGCH.
  - 3: Crea un slot con el SDCCH.
- "Datos entrada": contiene un Array de bits con los datos que se quieren incluir en la ráfaga normal, como es el caso del AGCH y el SDCCH.
- "Input Complex Waveform": este parámetro contiene una forma de onda a la que se le añade la nueva forma de onda correspondiente al slot creado. De esta forma se pueden concatenar las formas de onda de los 8 slots que se crean y conseguir la forma de onda de la trama.
- "TSC (Normal Burst)": este parámetro es necesario para pasárselo al bloque "Burst.vi" que se explicó anteriormente.
- "Session handle in": esta entrada no se modifica y sale tal cual: Esto es así porque, como se verá luego, es un parámetro de configuración del USRP-2920.

Por otro lado existen dos salidas, "Output Complex Waveform" que contiene la forma de onda que sale del bloque, y "Session handle out" que como se dijo anteriormente es la entrada "Session handle in" sin modificaciones.

Este bloque es uno de los más importantes del programa, ya que en él se incluyen la mayoría de los VI que hemos visto hasta ahora.

5.2.6. Envío y recepción de las tramas

Tanto el envío como la recepción de las tramas se realizan a través de los USRP-2920, cuya configuración en LabVIEW se explica en este apartado.

En el caso de la emisión se ha creado un VI denominado "Configuración emisor.vi" que se encarga de la configuración y puede verse en las Figuras 40 y 41.

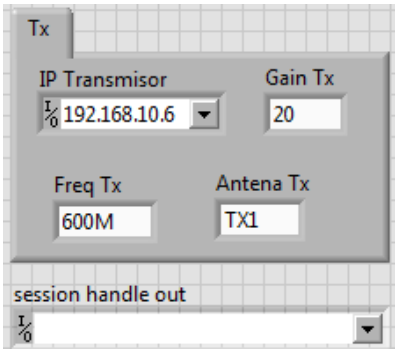

Figura 40: "Configuración emisor.vi" (Panel frontal)

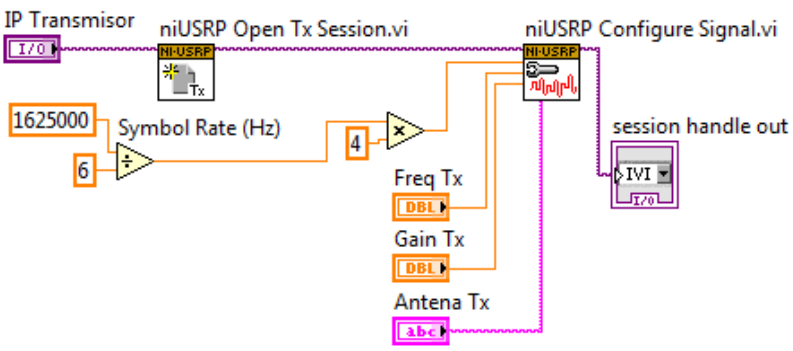

Figura 41: "Configuración emisor.vi" (Diagrama de bloques)

En este módulo se puede ver cómo se inicia y se configura una sesión del USRP-2920, para lo que hace falta indicar la dirección IP del transceptor ("IP Transmisor"), la ganancia que se quiere tener ("Gain Tx"), la frecuencia en la que se quiere transmitir ("Freq TX") y la antena del USRP-2920 que se usa ("Antena Tx"). También es necesario indicar la tasa de símbolo que se requiere, que en este caso será la tasa de GSM (270,83 kbps o 1625/6 kbps) multiplicado por 4 para tener 4 muestras por símbolo.

La salida de este VI es "session handle out", que lleva todos los parámetros de la configuración. Por último, esta salida debe usarse como entrada a un último bloque que viene implementado en LabVIEW y que, junto con la forma de onda que se quiere transmitir, constituye todo lo necesario para que el USRP-2920 comience la transmisión.

En cuanto a la recepción, es parecida a la emisión pero requiere de algún parámetro más que configurar. El VI encargado de la configuración del receptor se ha denominado "Configuración receptor.vi" y se muestra en las Figuras 42 y 43.

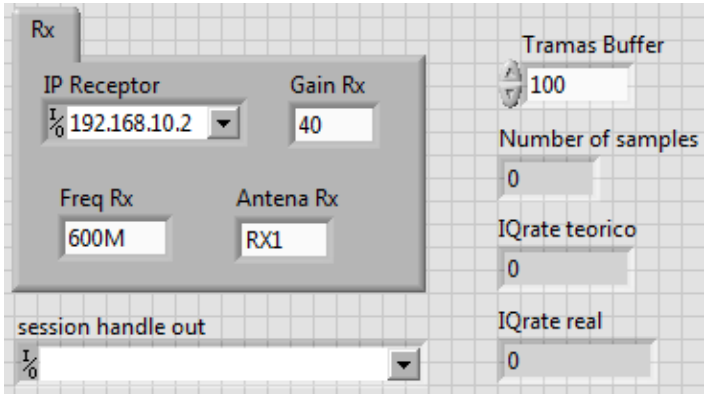

Figura 42: "Configuración receptor.vi" (panel frontal)

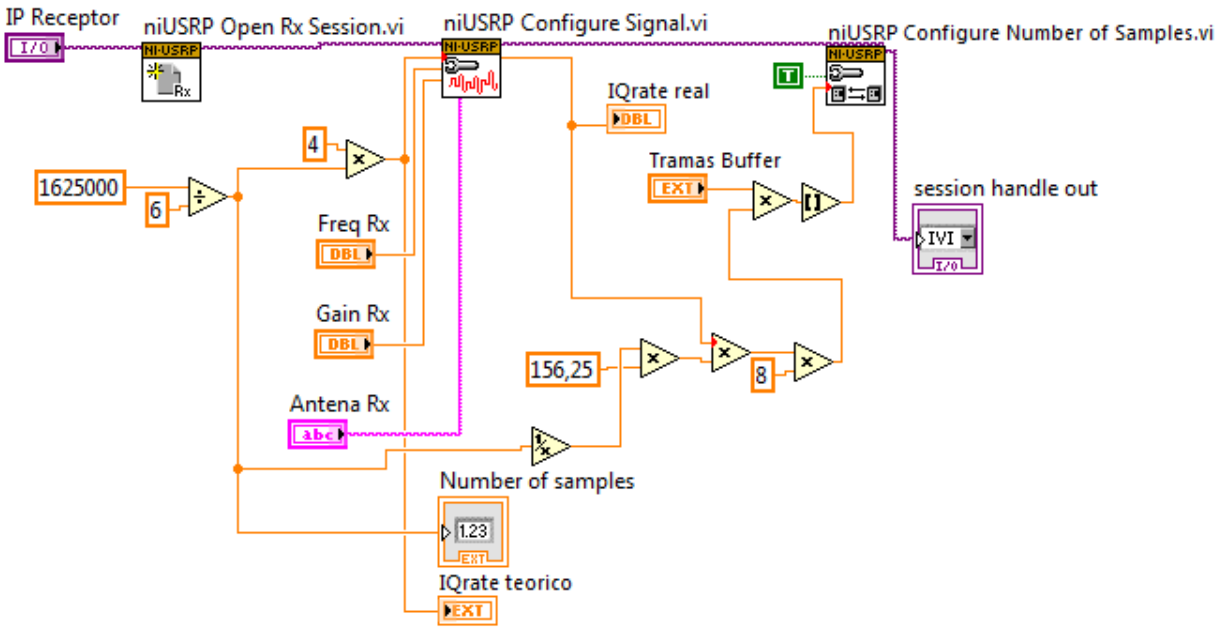

Figura 43: "Configuración receptor.vi" (Diagrama de bloques)

El proceso seguido aquí es igual que en el emisor, siendo la única excepción la inclusión de un bloque al final ("niUSRP Configure Number os Samples.vi") en el que se determinan las muestras a tomar en la recepción. Por tanto, la única entrada que se le añade con respecto a la configuración del emisor es "Tramas buffer", que se encarga de indicar el número de tramas (muestras correspondientes a una trama) que se quieren recoger.

Como pasaba con el emisor, tras esta configuración, la salida "session handle out" se pasa como entrada a otro bloque que se encarga de comenzar la recepción de las muestras indicadas y obtener una onda que será la entrada del demodulador.

5.2.7. Demodulación

Para realizar la demodulación en este trabajo se han utilizado 2 VI, uno dentro de otro. Lo que se consigue con estos bloques es transformar la onda que tiene como salida el bloque receptor del USRP-2920 en un Array de bits. Como se comentó anteriormente, en este trabajo no se realiza una comunicación exactamente igual que en GSM, ya que en el estándar existe una sincronización que en este caso no se implementa.

El bloque que se usa para recibir la onda y devolver el Array de bits se ha llamado "Demodulador.vi" y puede verse en la Figura 44.

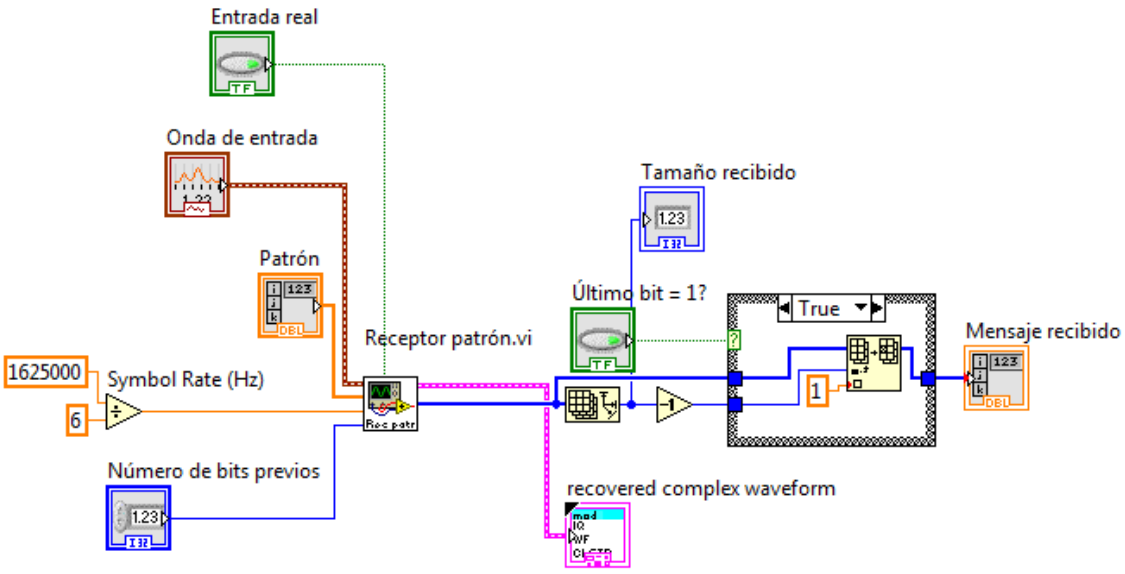

Figura 44: "Demodulador.vi"

Las entradas y salidas de este bloque están todas conectadas a "Receptor patrón.vi", núcleo de "Demodulador.vi" y encargado de realizar la demodulación en sí. La función de este bloque, por tanto, consiste en pasar los parámetros necesarios a "Receptor patrón.vi" con la configuración adecuada, y realizar alguna pequeña corrección a la salida en caso de ser necesario.

El bloque "Receptor patrón.vi" se muestra en la Figura 45.

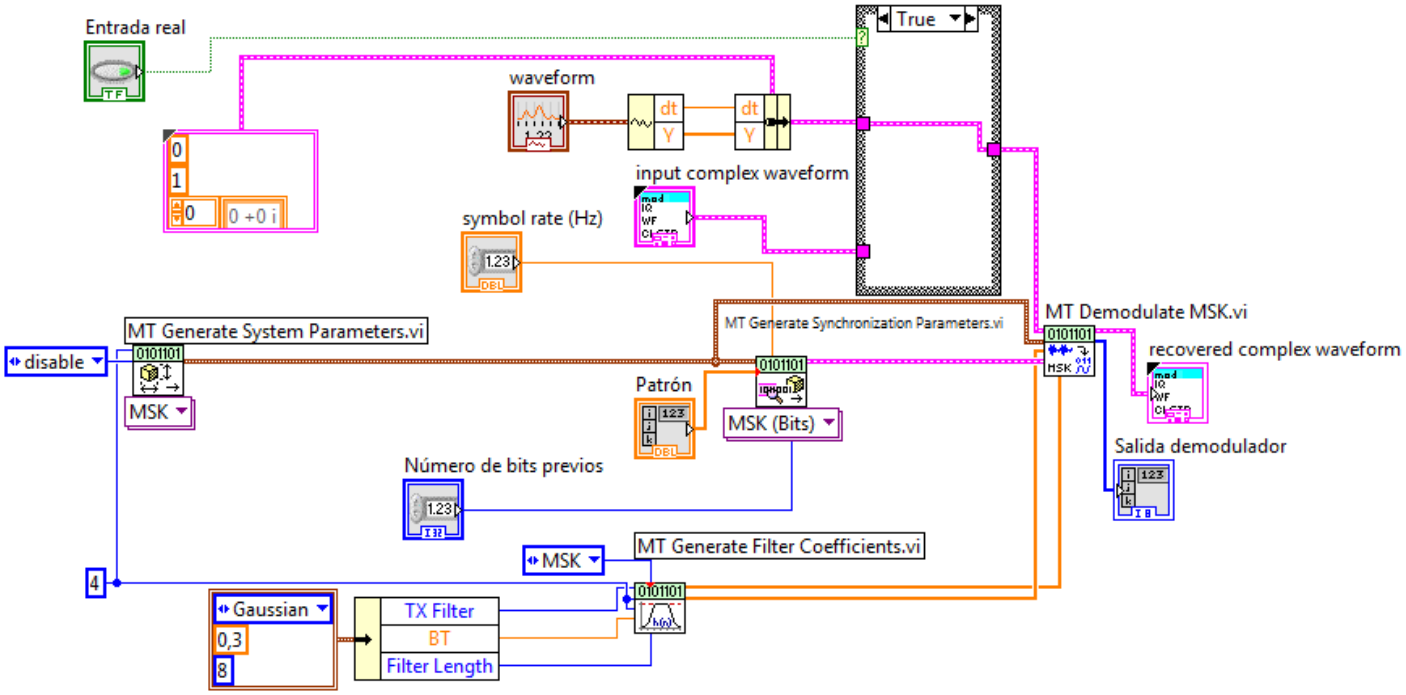

Figura 45: "Receptor patrón.vi"

Como se dijo antes, este bloque es el encargado de realizar la demodulación cogiendo la entrada "waveform" y obteniendo la salida "Salida demodulador". Más concretamente, en este bloque se utilizan los módulos que vienen implementados en LabVIEW para configurar el demodulador de forma que se realice una demodulación GMSK.

Otras dos entradas importantes que tiene este bloque son "Patrón" y "Número de bits previos". Su importancia radica en que se utilizan para que en el Array de bits de salida se encuentre el patrón indicado (la "Synch. Sequence Bits" en el caso de la ráfaga de acceso y la "Training Sequence" en el caso de la ráfaga normal), y que comience en la posición dada en "Número de bits previos". De esta forma, aunque no se realice la sincronización real de GSM, es posible obtener en la salida un Array de bits que comience por el mensaje que se espera recibir.

5.2.8. Obtención de los mensajes

Una vez realizada la demodulación es necesario obtener la ráfaga transmitida para poder conseguir el mensaje original. Este proceso se realiza en dos VI, uno encargado de recibir una ráfaga y conseguir el mensaje codificado, y otro encargado de recibir este mensaje codificado y obtener el original.

Sin embargo, antes de pasar por este proceso es necesario sacar la ráfaga de 148 bits. Para ello sólo es necesario conseguir los primeros 148 bits del Array que sale del demodulador ya que, como se vio, estos ya salían ordenados.

Para deshacer la ráfaga se utiliza el bloque "Deshacer burst.vi" que se muestra en las Figuras 46 y 47.

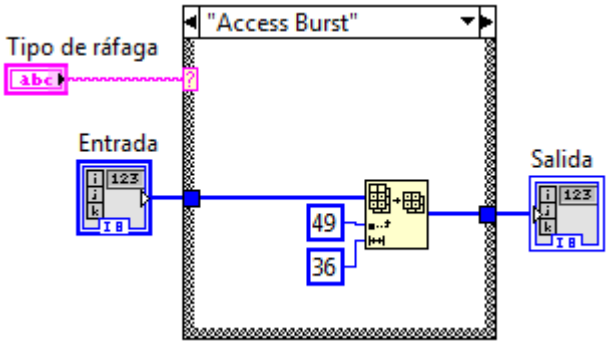

Figura 46: "Deshacer burst.vi" (Access Burst)

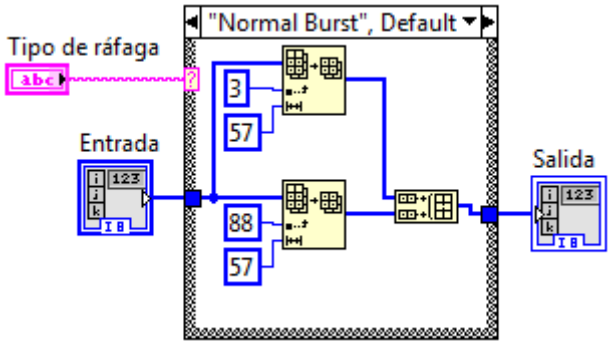

Figura 47: "Deshacer burst.vi" (Normal burst)

Las entradas de estos bloques son:

- "Tipo de ráfaga": es un String en el que se indica si la ráfaga de entrada es una ráfaga de acceso o una ráfaga normal.
- "Entrada": son los 148 bits que componen la ráfaga.

Por otra parte, solo existe una salida ("Salida"), y son los bits del mensaje incluido en la ráfaga. Estos bits son 36 en el caso de la ráfaga de acceso y 114 en el caso de la ráfaga normal.

En cuanto a la decodificación, se ha creado un VI para cada canal lógico, el primero es "RACH decoding.vi", que se muestra en la Figura 48.

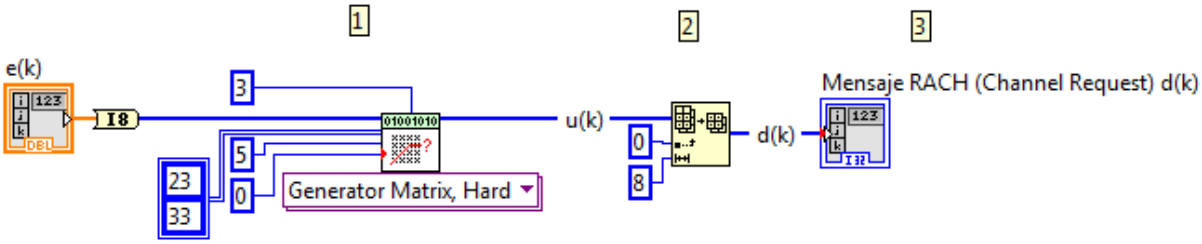

Figura 48: "RACH decoding.vi"

En este bloque se realiza el proceso contrario que en el codificador, recibiendo la entrada de 36 bits "e(k)", y obteniendo los 8 bits del mensaje original en la salida "Mensaje RACH (Channel Request) d(k)" .

En el punto 1 se deshace la codificación convolucional del codificador y se obtienen 18 bits y, tras esto, se cogen los 8 primeros bits (punto 2) que corresponden al mensaje original (punto 3).

La decodificación del AGCH y del SDCCH es igual, y no presenta muchas diferencias con la del RACH. La principal diferencia está en las entradas, ya que en este caso se reciben 4 grupos de 114 bits (i(B,j)) y se unen en una matriz de 4x114, para después pasar por el proceso inverso al entrelazado que se producía en el codificador.

Los VI encargados de realizar este procesos se han denominado "AGCH decoding.vi" (Figura 49) y "SDCCH decoding.vi".

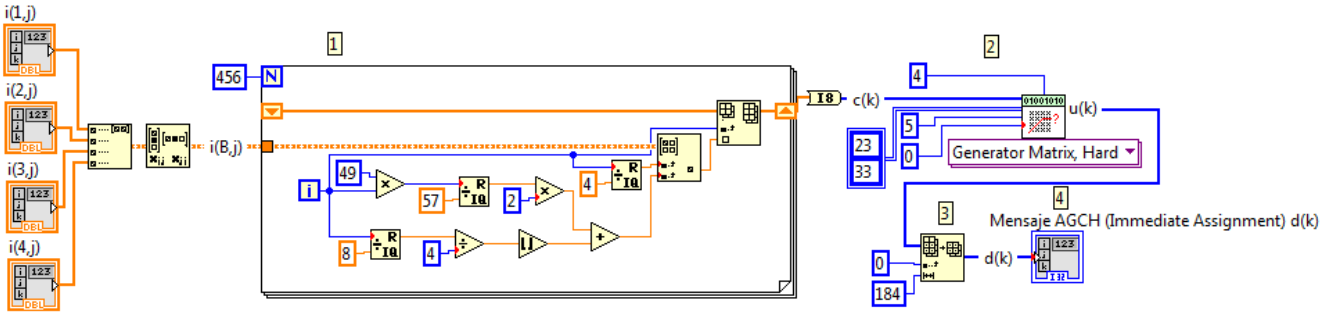

Figura 49: "AGCH decoding.vi"

Como se ve, en el paso 1 se forma la matriz de 4x114 y se deshace el entrelazado, tras esto se obtiene el Array "c(k)" con 456 bits que, en el paso 2, se hacen pasar por el proceso inverso al codificador convolucional, luego (en el paso 3) se cogen los 184 bits correspondientes al mensaje original (paso 4). Estos 184 bits son la salida del bloque "Mensaje AGCH (Immediate Assigment) d(k)".

5.3. Diseño del programa final

Ya se ha explicado el funcionamiento de los módulos que forman parte del programa, por lo que el paso final es juntarlos todos de forma adecuada para completar el procedimiento que se simula en el trabajo.

El programa final está dividido en dos partes, por un lado está el VI encargado de simular el funcionamiento de la estación móvil (llamado "MS.vi"), y por otro el que simula el funcionamiento de la estación base (llamado "BTS.vi"). Ambos son prácticamente iguales, cambiando solo los mensajes que envían y que esperan recibir.

Como se dijo en el capítulo 4, el programa requiere dos ordenadores y cuatro transceptores para funcionar correctamente. Un ordenador y dos transceptores hacen el papel de la estación móvil y otro ordenador con otros dos transceptores simulan la estación base.

5.3.1. Estación Móvil (MS)

Este bloque hace las funciones de la estación móvil dentro de la comunicación, para lo cual realiza los siguientes pasos:

- Lo primero que se realiza es una configuración, tanto del emisor como del receptor, con los bloques vistos anteriormente en este capítulo.
- Tras esto, se comienza a emitir el "Channel Request" a través del RACH usando el slot tres de una ráfaga. La emisión es continua, estando en un bucle a la espera de recibir el "Immediate Assigment" para parar la transmisión y comenzar con el siguiente mensaje.
- A su vez, el receptor comienza esperando recibir el "Immediate Assigment" que tiene que enviar la BTS cuando reciba el "Channel Request". Para la recepción, se comprueban los datos recibidos usando como patrón la TSC de la ráfaga (se utiliza la

tercera), de forma que cuando la secuencia es detectada se toman los 148 bits correspondientes a una ráfaga y se comprueba que el mensaje es el esperado. Si es así, se pasa a comprobar el siguiente mensaje de la misma forma. Esto se hace cuatro veces hasta que se reciben las cuatro partes del mensaje esperado y pasan por el proceso de decodificación explicado previamente. De esta forma se obtiene el mensaje original mandado por la BTS.

- Cuando se recibe la primera parte del mensaje "Immediate Assigment" se para la transmisión del "Channel Request" y se comienzan a enviar tramas vacías. Esto sucede hasta que se recibe la cuarta parte del mensaje y, en ese momento, se comienza a enviar el "Location Updating Request" a través del SDCCH. Como el mensaje se ha de transmitir en cuatro slots, se concatenan cuatro tramas en las cuales se usa el tercer slot como contenedor de cada una de las partes.
- Por otro lado, cuando en el receptor se obtiene la cuarta parte del mensaje "Immediate Assigment", este comienza con recepción del "Location Updating Accept" de la misma forma que antes.
- Una vez que se recibe el primer mensaje del "Location Updating Accept" se para la transmisión del "Location Updating Request" y se envían tramas vacías. Al recibir la cuarta parte del mensaje se comienza a transmitir el "Channel Release".
- Al mismo tiempo, el receptor ya está esperando la última parte del "Location Updating Accept" para empezar la recepción del "TMSI Reallocation Complete".
- Cuando se recibe el primer mensaje del "TMSI Reallocation Complete" el transmisor se para y se da por finalizada su labor.
- Por último, el receptor sigue funcionando hasta que recibe el cuarto mensaje del "TMSI Reallocation Complete", momento en que para y se da por finalizado el procedimiento.

Para que se entienda mejor, el funcionamiento del VI "MS.vi" se ilustra en la Figura 50.

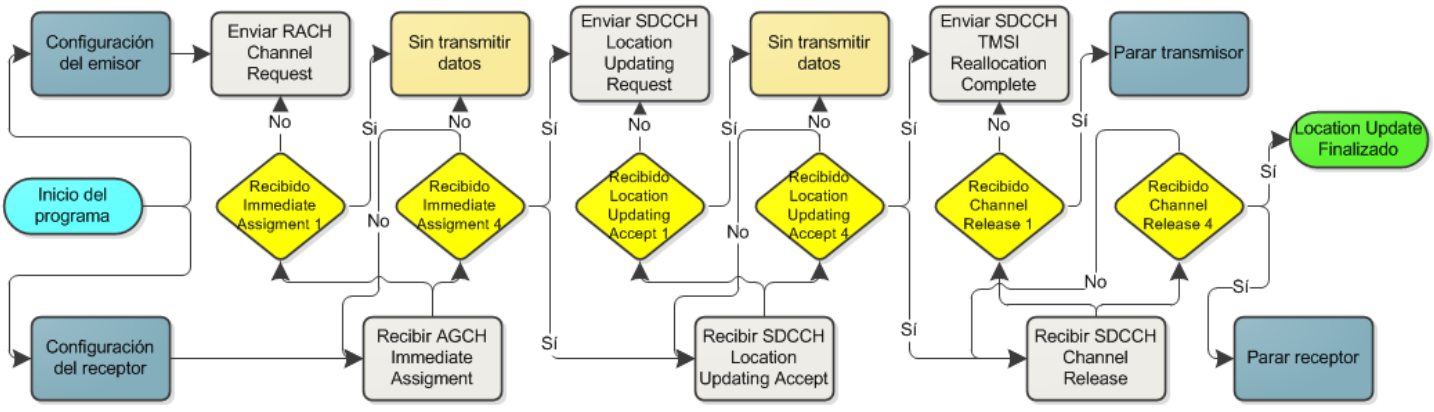

Figura 50: Esquema de funcionamiento del bloque "MS.vi"

En el programa se ignoran los mensajes relativos a la autenticación y al cifrado ya que, aunque se expusieron teóricamente y se implementaron en un bloque, no son de mucha importancia en el proceso y solo servirían para complicar el funcionamiento del programa.

En la Figura 51 se puede ver el aspecto de la interfaz de usuario, en la que se ilustra el estado del procedimiento gracias a indicadores que se van encendiendo a medida que se reciben los mensajes. También se indica qué está haciendo el emisor y el receptor en cada momento, cuantas transmisiones y recepciones se han producido, el mensaje que se está enviando, el que se está recibiendo, el patrón usado en la recepción y sus respectivos tamaños. Además, es posible configurar el número de tramas que se quieren obtener en cada recepción, así como los parámetros de configuración de los transceptores usados.

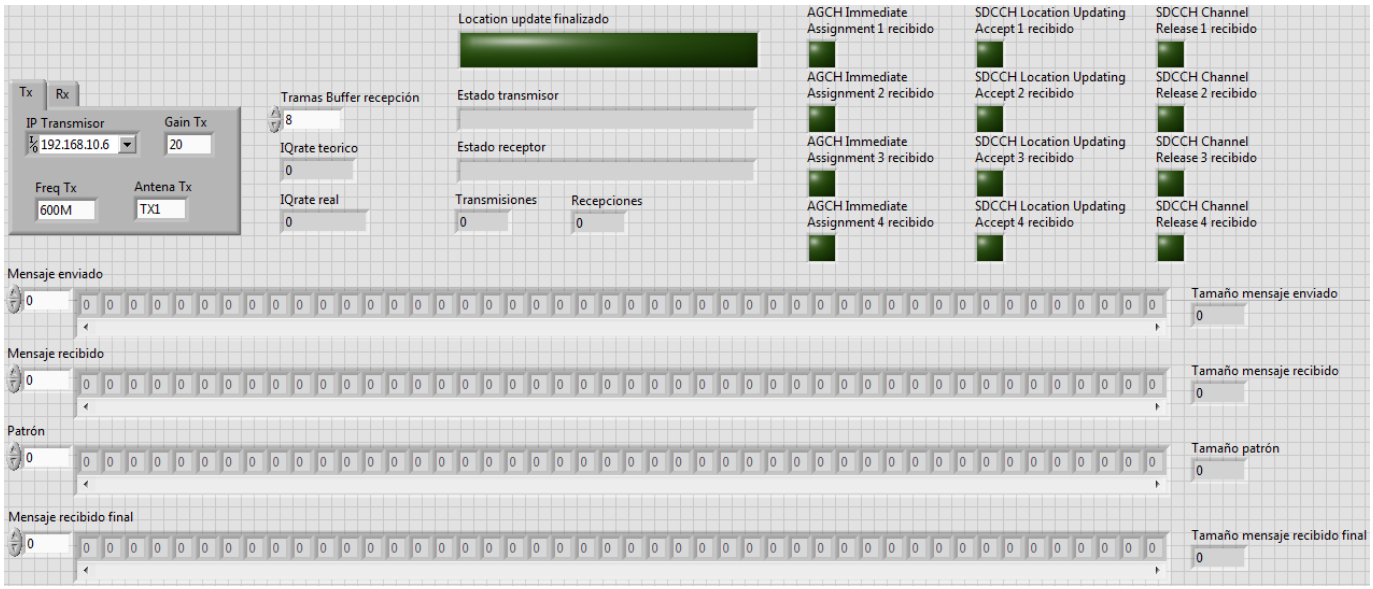

Figura 51: "MS.vi" (Panel Frontal)

5.3.2. Estación Base (BTS)

Este bloque hace las funciones de la estación base, y su funcionamiento es análogo al que se ha explicado en la estación móvil. El proceso seguido es el siguiente:

- Se configuran el transmisor y el receptor con los parámetros necesarios.
- Antes de transmitir nada, el receptor está esperando el “Channel Request” procedente de la estación móvil.
- Cuando se recibe el mensaje, el transmisor comienza a enviar en “Immediate Assigment” a través del AGCH y el receptor pasa a esperar la llegada del “Location Updating Request”.
- Cuando se recibe la primera parte del “Location Updating Request”, el transmisor para la emisión del “Immediate Assigment” (ya que este ya ha sido recibido por el móvil) y envía tramas vacías.
- Por su parte, el receptor sigue esperando hasta obtener la cuarta parte del “Location Updating Request”. Cuando esto ocurre, el transmisor comienza el envío del “Location Updating Accept” y el receptor pasa a esperar el “TMSI Reallocation Complete”.
- Cuando se recibe la primera parte del “TMSI Reallocation Complete”, el transmisor para la emisión del “Location Updating Accept” y envía tramas vacías.

- A su vez, el receptor espera la llegada de la cuarta parte del "TMSI Reallocation Complete". Cuando esto sucede el receptor se para y da por finalizada la recepción. Además, el emisor comienza a transmitir el "Channel Release".
- Por último, como en este ejemplo la BTS no tiene forma de saber cuándo el mensaje ha sido recibido por parte del móvil, se ha añadido en la interfaz de usuario un botón que ha de pulsarse cuando eso ocurra para parar la transmisión y dar por finalizado el procedimiento.

Para que se entienda mejor, el funcionamiento del VI "BTS.vi" se ilustra en la Figura 52.

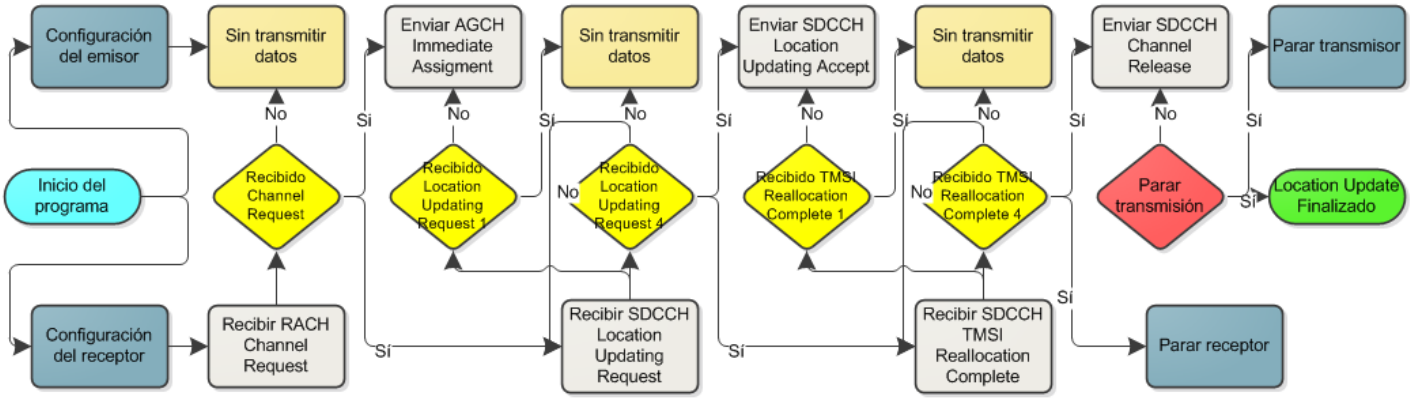

Figura 52: Esquema de funcionamiento del bloque "BTS.vi"

En cuanto a la interfaz de usuario (Figura 53), es igual que la del móvil, con la diferencia de que se le ha añadido el botón comentado anteriormente para parar la transmisión, y que el nombre de los indicadores ahora es el correspondiente a los mensajes esperados por la estación base.

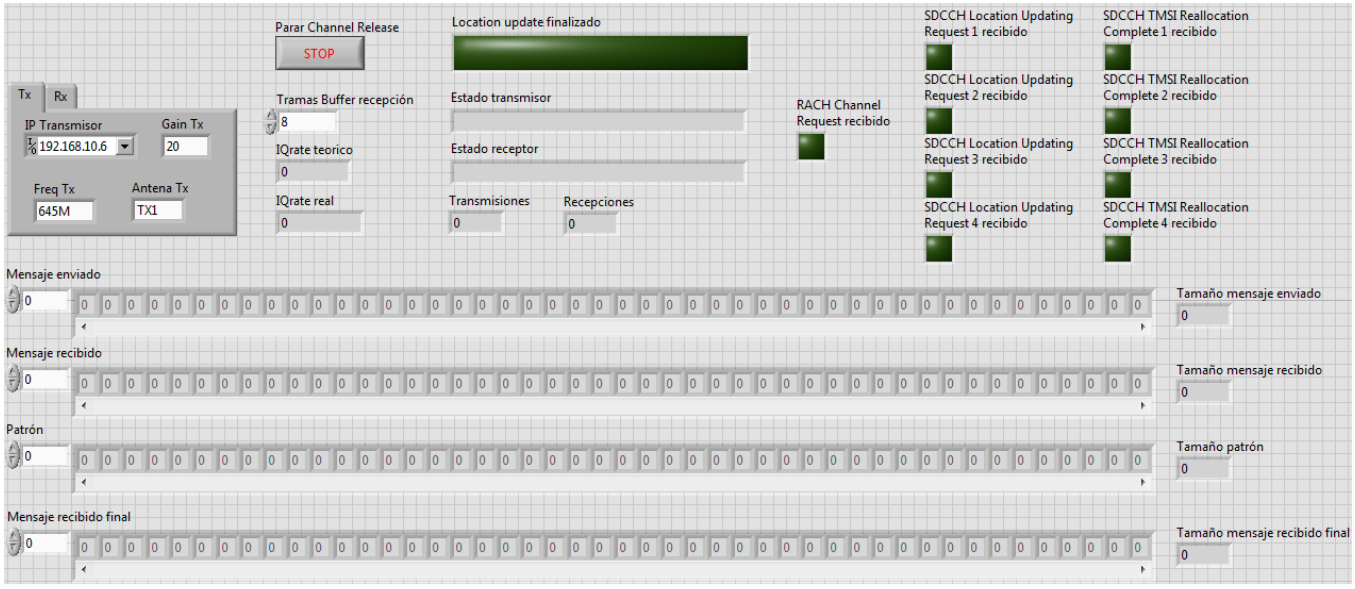

Figura 53: "BTS.vi" (Panel frontal)

6. Pruebas y comprobaciones

Durante la realización del TFG, todos los módulos de los que consta el programa se han ido probando a medida que se iban completando. De esta forma, se pretendía ir desarrollando el mismo con una buena base, evitando errores en pasos previos una vez estuviera más adelantado. Lo que se expone a continuación son algunas de las comprobaciones que se han realizado durante el desarrollo del trabajo.

6.1. Codificación y decodificación

Las primeras pruebas realizadas se centran en los bloques de codificación. Lo que se hace principalmente es comprobar el tamaño del Array de bits en cada parte del procedimiento, para ver que es el esperado y se ajusta a las especificaciones. La parte del entrelazado del SDCCH y el AGCH es una de las más importantes, y para comprobar que se ejecuta de forma correcta, lo que se hace es ir comprobando explícitamente que la salida de este paso coincide con lo que se indica en la Tabla 1 del documento "GSM 05.03 - Channel coding" [35].

Además, para comprobar que los decodificadores están bien implementados, lo que se hace es concatenar un codificador con su correspondiente decodificador, y ver si la entrada y la salida son iguales.

6.2. Modulación y demodulación

Para la comprobación de la modulación y la demodulación se crea un VI específico en el que se junta la modulación y la demodulación, introduciendo un Array de bits y un patrón para ver si se encuentra el patrón y la salida es igual a la entrada. El VI creado para esto se ha denominado "Prueba modulación", y puede verse un ejemplo del resultado de su ejecución en la Figura 54.

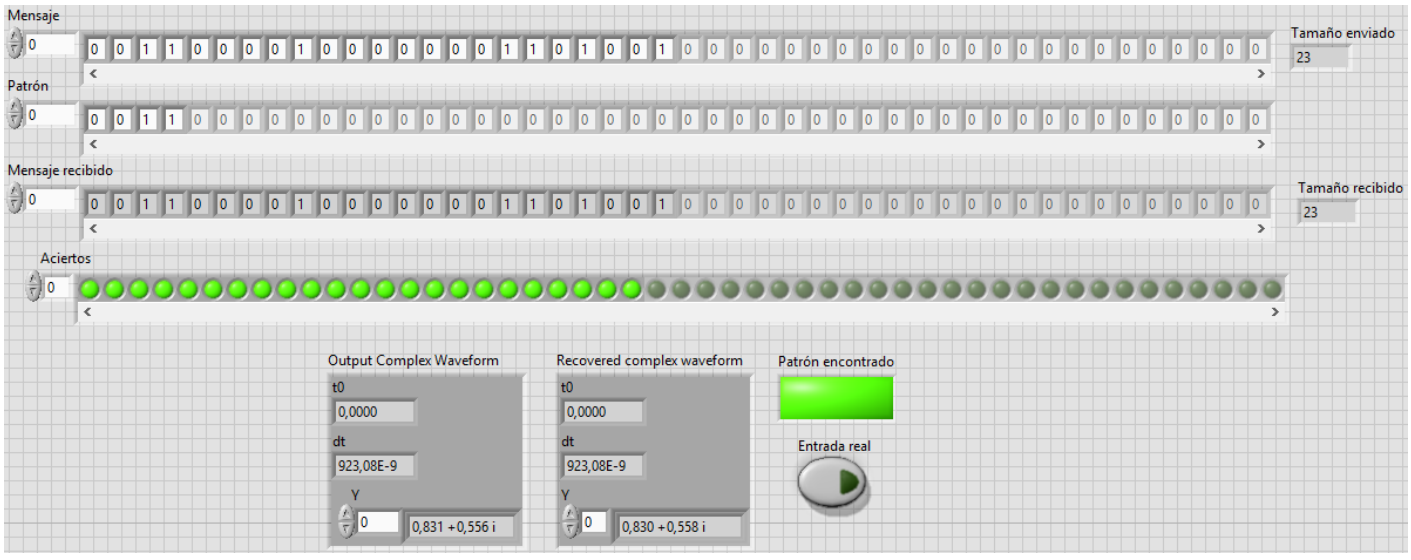

Figura 54: "Prueba modulación.vi" (Panel frontal)

6.3. Programa final

Las pruebas realizadas sobre el programa final son las más importantes ya que de ellas depende el éxito del trabajo. Aunque este último programa supone una comprobación en sí mismo, ya que en él se usan todos los bloques implementados, se realizan algunas pruebas adicionales para ver si se obtiene lo esperado.

Lo primero, aunque es un poco básico, es comprobar que la comunicación se realiza en las frecuencias deseadas que, como ya se comentó, son 600 MHz para el enlace de subida y 645 MHz para el de bajada. Para comprobar esto se usa el analizador de señales Agilent VSA 89600 que indica que todo es correcto como se puede ver en las Figuras 55 y 56.

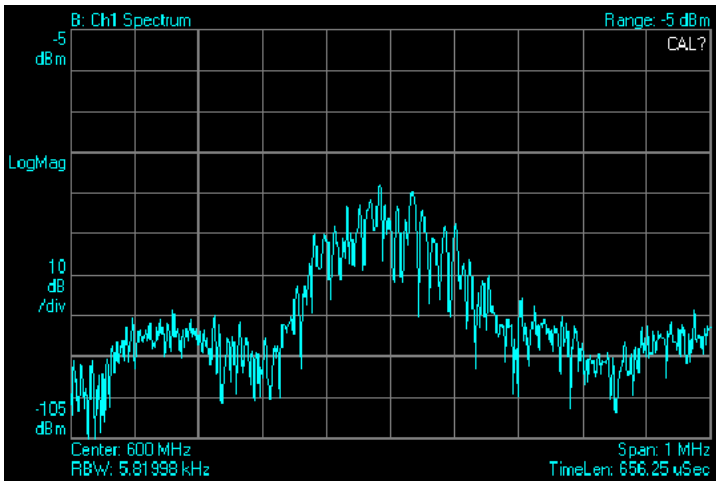

Figura 55: Enlace ascendente

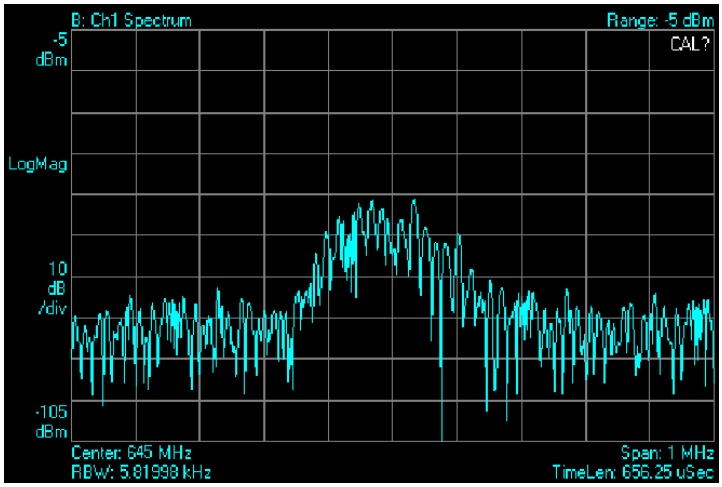

Figura 56: Enlace descendente

Otra comprobación hecha con el analizador de señales consiste en ver de forma gráfica cómo de diferentes son la ráfaga de acceso y la ráfaga normal. Como se vio, la ráfaga de acceso contenía menos información que las demás, ya que su periodo de guarda era mucho mayor. En las Figuras 57 y 58 se puede ver esta diferencia. Además, también se puede comprobar como en una trama se envía una sola ráfaga quedando el resto vacías.

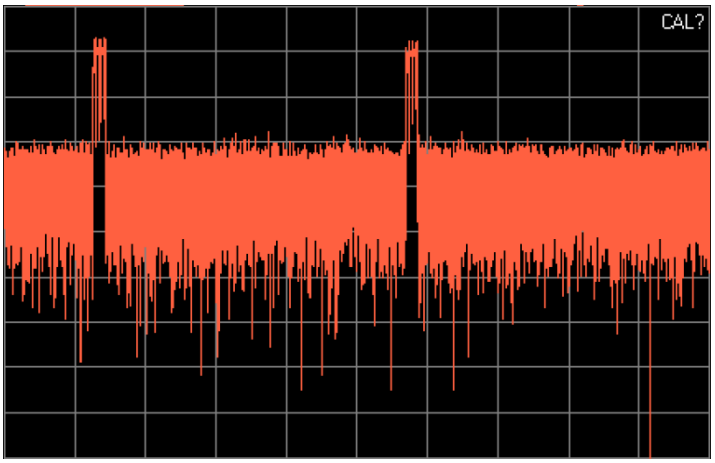

Figura 57: Ráfagas de RACH

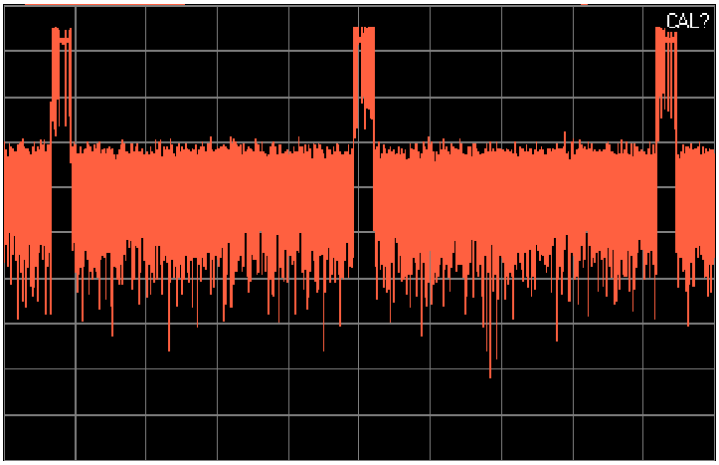

Figura 58: Ráfagas del SDCCH

Tras ver que en teoría la transmisión y la recepción en la interfaz radio tiene la forma esperada, se pasa a ejecutar el programa para ver si funciona como se espera. Para comprobarlo se ejecutan ambos VI (“MS.vi” y “BTS.vi”) a la vez, de forma que la estación móvil comienza enviando el “Channel Request” y esperando el “Immediate Assigment”, y la estación base espera el “Channel Request”. En las Figuras 59, 60, 61, 62, 63 y 64 se puede ver parte del proceso y cómo finalmente se completa todo el procedimiento.

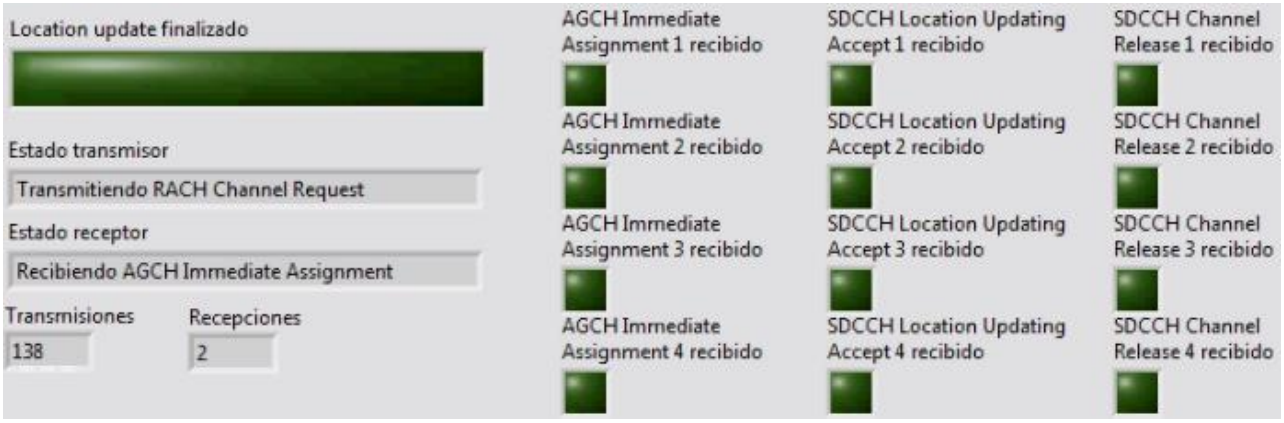

Figura 59: "MS.vi" Comienzo del proceso

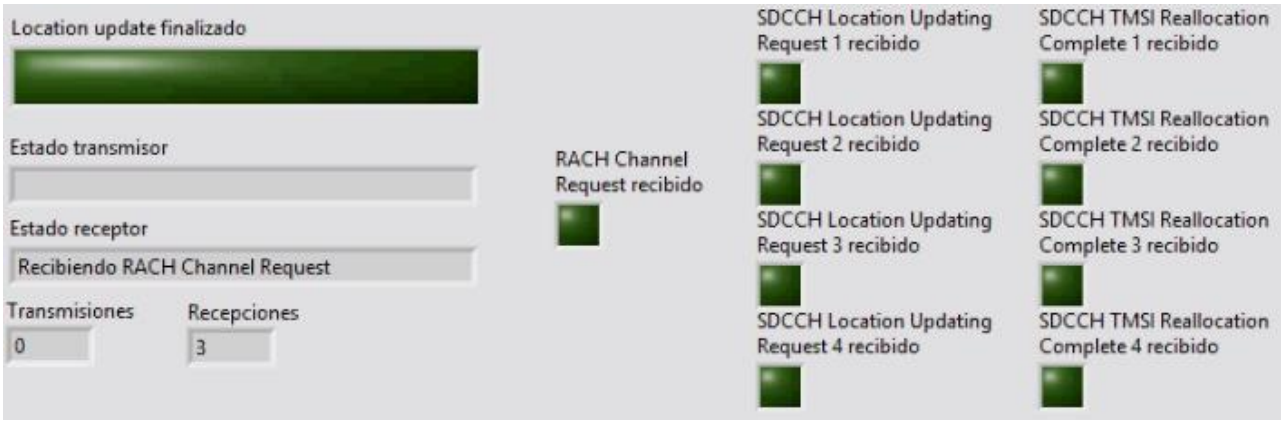

Figura 60: "BTS.vi" Comienzo del proceso

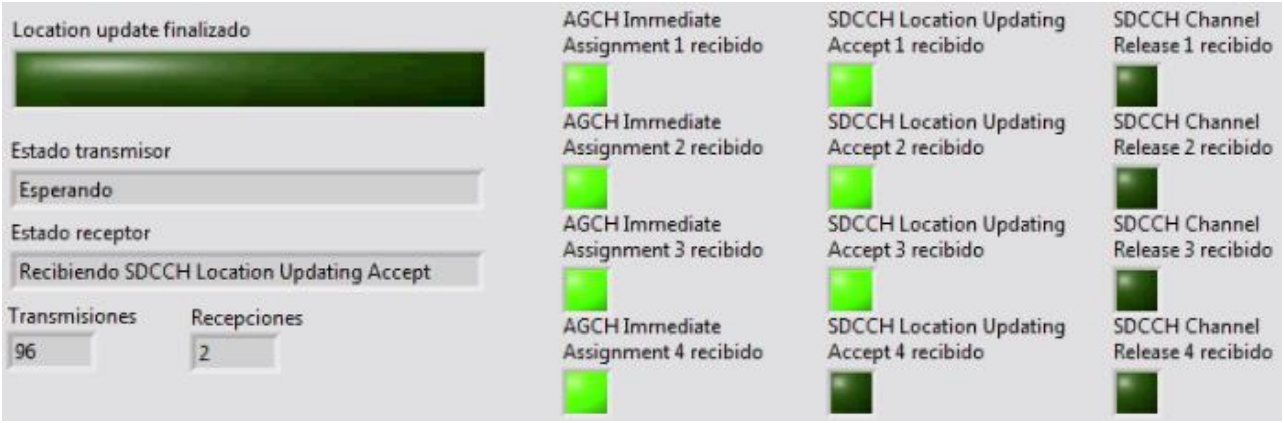

Figura 61: "MS.vi" Parte intermedia del proceso

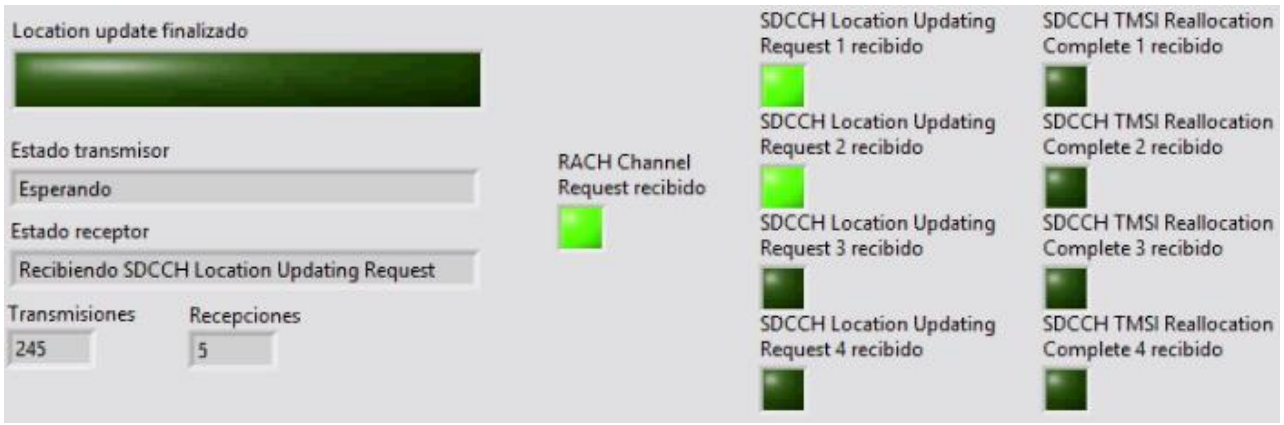

Figura 62: "BTS.vi" Parte intermedia del proceso

Figura 63: "MS.vi" Finalización del proceso

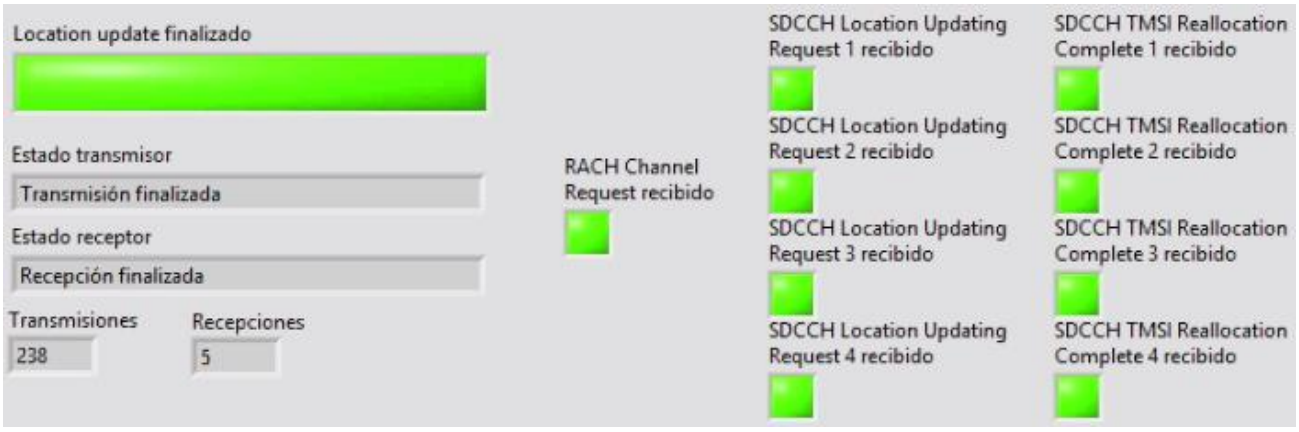

Figura 64: "BTS.vi" Finalización del proceso

Con esto se pueden dar por concluidas las pruebas y afirmar que el programa cumple con las expectativas.

7. Conclusiones

7.1. Versión en español

Como se ha comentado en múltiples ocasiones, el objetivo principal de este trabajo era ilustrar el proceso que se lleva a cabo cuando un móvil cambia su zona de cobertura en GSM. Este proceso lleva consigo una serie de pasos, los cuales han sido implementados siguiendo el estándar en la medida de lo posible.

Para completar el desarrollo se decidió realizar dos interfaces de usuario, una que representa a la estación móvil y otra que representa a la estación base. De esta forma, se pueden ejecutar en dos ordenadores diferentes y comprobar que realmente están enviando y recibiendo los mensajes como es debido. En ambas interfaces se pueden elegir distintos parámetros de la comunicación aunque, al realizarse un proceso muy concreto, hay muchos otros que son fijos. Sin embargo, algunos parámetros que no son manipulables desde la interfaz principal (como los campos de los mensajes), pueden ser cambiados con pequeñas modificaciones del código que cualquier persona sin conocimientos de LabVIEW podría realizar.

En cuanto a las herramientas usadas en el proyecto, aunque no se tenían conocimientos previos de cómo funcionaban, ha sido fácil acostumbrarse. Además, la realización de este trabajo ha servido al alumno para adquirir nuevos e interesantes conocimientos acerca de la tecnología SDR y del funcionamiento de GSM.

Del funcionamiento del programa desarrollado se puede decir que cumple los requisitos propuestos. Aunque ya se ha visto que hay partes del estándar, como la sincronización, que no se han podido implementar por su dificultad, la mayor parte del proceso sí se desarrolla según el funcionamiento original de GSM. Por tanto, se puede decir que el programa cumplirá su objetivo de servir como ejemplo a otros estudiantes acerca de cómo funciona esta parte concreta de GSM.

Por otro lado, este trabajo deja abierto un gran número de futuras líneas de trabajo posibles. Como ejemplo de lo que se puede hacer para completar o ampliar el trabajo hecho tenemos:

- El desarrollo de la sincronización real que se da en GSM, de forma que la comunicación tenga más sentido y permita implementar multitud de funciones adicionales.
- Agregar al proceso realizado una segunda estación base para ver cómo se produce el "Location Update" en la realidad. Así se podría observar que cuando el móvil recibe una mejor señal de la segunda estación base inicia el proceso aquí implementado.
- El desarrollo de nuevos procedimientos de GSM que utilicen otros mensajes y canales a los usados en esta ocasión. Esto permitiría ampliar el desarrollo del estándar en la plataforma SDR y conseguir, en un futuro, la simulación de gran parte del funcionamiento de GSM.

7.2. English version

As has been discussed in many times, the main objective of this project was to show the process that takes place when a mobile phone changes his base station in GSM. This process needs to follow some steps, which have been implemented following as far as possible the standard.

To complete this development it was decided to create two different user interfaces, one of them represents the MS (Mobile Station) and the other one represents the BTS (Base Transceiver Station). This way it is possible to execute them in two different computers and see that they are sending and receiving the messages as they should. In both interfaces there are different communication parameters to choose, although as it is a concrete process, there are many others that can't change. However, some of the parameters that can't be manipulated in the user interface (such as the message elements) can be easily changed with minor modifications of the code by anybody without previous knowledge about LabVIEW.

As to the tools used in the project, although the student didn't have any previous knowledge about his performance, it was easy to get used. In addition, the completion of this project has helped the student to get new and interesting knowledge about the SDR technology and the GSM workings.

It can be said that the developed program workings achieves the proposed requirements. As it was mentioned before, there are some parts of the standard (such as the synchronization) which couldn't be implemented cause of his difficulty, but most of the processes are implemented following the original GSM workings. Therefore, we can say that the program will accomplish its goal of serving as an example to other students about how this particular GSM part works.

Furthermore, this project has a large number of possible future work lines. Some examples of them are the next:

- The development of the real synchronization that takes place in GSM, so that communication makes more sense and allows implementing many additional functions.
- Add a second BTS to the already done project in order to see how the "Location Update" process is started by the MS when it receives a better signal from this second BTS.
- The development of new GSM procedures which use another messages and channels. It would allow extending the development of the standard in the SDR platform and get, in the future, the simulation of most of the running of GSM.

Anexos

A. Planificación

El proyecto fue asignado en el mes de diciembre de 2014 y se comenzó a trabajar el día 1 del mes de febrero de 2015. Desde ese momento, el tiempo dedicado al mismo ha sido constante y diario, excluyendo fines de semana y días festivos, siendo estos últimos los siguientes: 19 de marzo; 2 y 3 de abril; 1 y 2 de mayo; 4 de junio; 17 de agosto. Finalmente, el trabajo se da por concluido el día 11 de septiembre de 2015.

Para una correcta planificación del trabajo se realiza una división en 6 etapas en función de lo que se realiza en cada una de ellas. Las etapas están divididas de la siguiente manera:

1. **Documentación y estudio del estándar GSM** (15 días).
   1.1. Búsqueda y recopilación de los documentos usados para comprender el funcionamiento de GSM (5 días).
   1.2. Estudio de los documentos recopilados que son necesarios para la implementación del trabajo (10 días).
2. **Aprendizaje y familiarización con las herramientas usadas** (22 días).
   2.1. Familiarización con el entorno de trabajo LabVIEW (18 días).
   2.2. Comprensión del funcionamiento del transceptor USRP-2920 (4 días).
3. **Realización del programa** (63 días).
   3.1. Programación de módulos complementarios necesarios para el desarrollo completo del programa (6 días).
   3.2. Creación de los mensajes necesarios en el procedimiento (5 días).
   3.3. Programación de los codificadores y decodificadores de los distintos canales usados en la comunicación (14 días).
   3.4. Organización de los mensajes y creación de tramas para su posterior envío (11 días).
   3.5. Programación del modulador y demodulador GMSK utilizado (17 días).
   3.6. Creación de la interfaz de usuario final (10 días).
4. **Pruebas y resultados** (21 días).
   4.1. Pruebas de los módulos complementarios (2 días).
   4.2. Pruebas de los codificadores y decodificadores (4 días).
   4.3. Pruebas de creación de tramas (3 días).
   4.4. Pruebas del modulador y el demodulador (5 días).
   4.5. Comprobación del correcto funcionamiento del programa final (7 días).
5. **Conclusiones finales** (3 días).
6. **Realización de la memoria** (30 días).

Todas las fases siguen un desarrollo lineal en el tiempo excepto las etapas 3 y 4, las cuales se ha ido complementando de forma que cada módulo nuevo que se programaba era probado antes de pasar al siguiente.

Por tanto, vemos como la duración total del trabajo es de aproximadamente 7 meses y medio, que deja un total de 154 días de trabajo, con una media de 2,5 horas por cada día. Para ilustrar de forma gráfica todo lo expuesto en este apartado se incluye un diagrama de Gantt con todo el desarrollo del trabajo en el tiempo.

Nombre de tarea	Duración	Comienzo	Fin
Trabajo Fin de Grado	**154 días**	**lun 02/02/15**	**vie 11/09/15**
1. Documentación y estudio del estándar GSM	**15 días**	**lun 02/02/15**	**vie 20/02/15**
1.1 Búsqueda y recopilación de documentos de GSM	5 días	lun 02/02/15	vie 06/02/15
1.2 Estudio de la documentación	10 días	lun 09/02/15	vie 20/02/15
2. Apredizaje y familiarización con las herramientas usadas	**22 días**	**lun 23/02/15**	**mié 25/03/15**
2.1. Entorno LabVIEW	18 días	lun 23/02/15	mié 18/03/15
2.2. Transceptor USRP-2920	4 días	vie 20/03/15	mié 25/03/15
3. Realización del programa	**79 días**	**jue 26/03/15**	**lun 20/07/15**
3.1. Programación de módulos complementarios	6 días	jue 26/03/15	lun 06/04/15
3.2. Creación de los mesajes	5 días	jue 09/04/15	mié 15/04/15
3.3. Programación de los codificadores y decodificadores	14 días	jue 16/04/15	mié 06/05/15
3.4. Organización de los mensajes	11 días	mié 13/05/15	mié 27/05/15
3.5. Programación del modulador y el demodulador	17 días	mar 02/06/15	jue 25/06/15
3.6. Creación de la interfaz de ususario	10 días	vie 03/07/15	jue 16/07/15
4. Pruebas y resultados	**78 días**	**mar 07/04/15**	**lun 27/07/15**
4.1. Pruebas de los módulos complementarios	2 días	mar 07/04/15	mié 08/04/15
4.2. Pruebas de los codificadores y decodificadores	4 días	jue 07/05/15	mar 12/05/15
4.3. Pruebas de creación de tramas	3 días	jue 28/05/15	lun 01/06/15
4.4. Pruebas del modulador y el demodulador	5 días	vie 26/06/15	jue 02/07/15
4.5. Pruebas del progama final	7 días	vie 17/07/15	lun 27/07/15
5. Conclusiones finales	**3 días**	**mar 28/07/15**	**jue 30/07/15**
6. Realización de la memoria	**30 días**	**vie 31/07/15**	**vie 11/09/15**

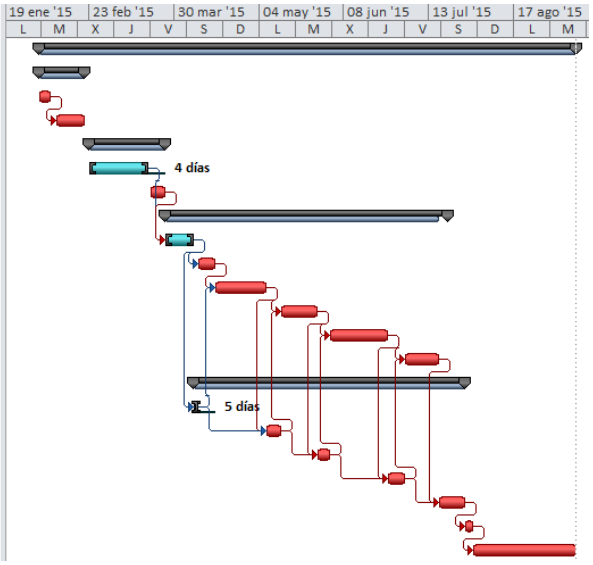

Figura 65: Diagrama de Gantt del proyecto

En el diagrama podemos observar en rojo las que serían las tareas críticas dentro de la planificación. Estas tareas son prácticamente todas, ya que se sigue un desarrollo muy dependiente entre ellas y para avanzar a la siguiente tiene que estar completa la previa.

B. Presupuesto

Para ver de forma detallada el presupuesto del trabajo se hará una división entre recursos materiales y humanos.

B.1. Recursos materiales

Para la realización del trabajo se han utilizado los siguientes elementos (detallados en el capítulo 4):

- Ordenador portátil Acer TravelMate 5760.
- Ordenador portátil ASUS A55A.
- Ordenador de sobremesa del laboratorio (para controlar el VSA).
- 4 x NI USRP-2920.
- 2 x Cable MIMO para NI USRP-2920.
- 4 x Antena para NI USRP-2920.
- NI LabVIEW 2014.
- Agilent VSA 89600S.

El coste que supone el uso de cada elemento se calcula con una amortización lineal dada por la siguiente fórmula:

$$\text{Amortización} = \frac{\text{Precio} \cdot \text{ Tiempo de uso}}{\text{Tiempo de amortización}}$$

El uso de cada componente no ha sido continuado, ya que hay algunos elementos que solo se han usado en las fases de pruebas intermedias y otros solo en la fase final de las pruebas. Concretamente, durante la fase de pruebas intermedias (toda la fase de pruebas excepto la prueba del programa final) se han usado dos transceptores USRP-2920, un cable MIMO y dos antenas, y durante las pruebas del programa final se usaron cuatro transceptores USRP-2920, dos cables MIMO, cuatro antenas y un segundo ordenador portátil. También se ha excluido del tiempo de uso del programa LabVIEW el periodo requerido para realizar la memoria y obtener las conclusiones finales, ya que durante este tiempo no fue necesario.

Para ver mejor cuanto tiempo se ha usado y qué coste supone cada elemento se ilustra el gasto en recursos materiales en la Tabla 13.

Concepto	Coste unitario	Cantidad	Tiempo de uso	Tiempo de amortización	Coste
Ordenador portátil Acer	464€	1 ud.	154 días	4 años	49,05€
Ordenador portátil Asus	599€	1 ud.	7 días (etapa de pruebas finales)	4 años	2.87€
NI USRP-2920	4740€	2 ud.	14 días (etapa de pruebas intermedias)	8 años	45,45€
		4 ud.	7 días (etapa de pruebas finales)		45,45€
Cable MIMO	150€	1 ud.	14 días (etapa de pruebas intermedias)	8 años	0,72€
		2 ud.	7 días (etapa de pruebas finales)		0,72€
Antena	100€	2 ud.	14 días (etapa de pruebas intermedias)	8 años	0,96€
		4 ud.	7 días (etapa de pruebas finales)		0,96€
NI LabVIEW	2920€	1 ud.	121 días	4 años	242,00€
Ordenador de sobremesa	1000€	1 ud.	21 (etapa de pruebas)	4 años	14,38€
Agilent VSA 89600S	165800€	1 ud.	21 días (etapa de pruebas)	15 años	635,95€
TOTAL					**1038,51€**

Tabla 13: Costes de materiales

B.2. Recursos humanos

En cuanto a los recursos humanos dedicados al trabajo se tiene en cuenta el tiempo empleado por el alumno de cuarto curso del Grado en Ingeniería en Tecnologías de Telecomunicación y el Doctor Ingeniero tutor del trabajo.

Concepto	Coste por hora de trabajo	Horas de trabajo	Coste
Doctor Ingeniero	75€/hora	30 horas	2250,00€
Estudiante	30€/hora	385 horas	11500,00€
TOTAL			**13750,00€**

Tabla 14: Costes de personal

B.3. Coste total

Finalmente, el coste total del trabajo se calcula sumando el coste de los recursos materiales y humanos (que representan los costes directos) y, además, hay que añadir los costes indirectos que se estima que suponen un 20% de los costes directos y el IVA (21%).

Concepto	Coste
Costes materiales	1038,51€
Costes humanos	13750,00€
Costes indirectos (20%)	2954,25€
Subtotal	17742,76€
IVA (21%)	3725,98€
TOTAL	**21468,74€**

Tabla 15: Coste total

C. Summary in English

A summary of the work will be done in this section, exposing the main ideas and the most important results.

C.1. Introduction

Since its inception, telecommunications systems have used specific hardware to work. However, some time ago appeared the concept of SDR (Software-Defined Radio), which gets replacing much of this hardware by software.

The work comes to complement a series of projects that has been proposed by the department of Signal Theory and Communications at the Carlos III University of Madrid to simulate the operation of some GSM [2] processes using the SDR technology. In this case it is intended to implement the "Location Update" procedure, which takes place when a mobile phone changes its coverage area and becomes to be managed by another base station.

This procedure involves exchanging a series of messages between the mobile phone and the new base station. The messages follow some steps since they are created until they are sent. In this paper these steps are implemented, as well as the exchange of messages over the radio interface.

C.2. Approach to work

In the last decades the world of mobile communications had advanced by leaps and bounds. However, it's possible that the most important revolution occurred with the introduction of GSM because it allows general people to enjoy this technology.

In addition, the SDR technology has grown in recent years and now there are many alternatives to implement in software what has always been made with hardware. Thus, just with an analog-digital converter and a RF adapter managed by a general purpose processor it is possible to develop mobile communications systems.

For this work, the SDR platform used is composed by NI USRP-2920 [8] transceivers and LabVIEW [7] software, both of them from National Instruments. Although there are alternatives such as *GNU Radio* [9] and *SDR-RADIO.com* [12], National instruments tools are used because they are the ones which are available in the workspace.

On the other hand, as this work is done in the university and it has teaching purpose, there isn't much to say about the socio-economic environment. Something similar happen with the regulatory framework, although there are certain laws and regulations relating to radio emissions which we must know, all the equipment placed on the laboratory where the work is developed fulfill this restrictions.

C.3. GSM standard

In this work a particular GSM procedure ("Location Update") is implemented. Therefore it is necessary to have some knowledge about how it functions.

First, it is important to note that GSM is a cellular system. The operation of these systems is based on the division of the area on which you want to give the service in cells. These cells are managed by a base station which covers its area. The cellular systems have benefits as good performance in coverage, capacity and spectrum use.

In terms of architecture, a GSM network consists of many components, however, in the developed project the most important components are the BTS ("Base Transceiver Station") and the MS ("Mobile Station"). The BTS handles the transmission and reception of the information in the radio interface. The MS is the user terminal, therefore, is the communication interface between the user and the radio network.

Regarding GSM radio interface, it is necessary to know how the messages are organized and sent. To understand how messages are organized, first thing is to know that the radio interface combines the frequency division access (FDMA/FDD) with the time division access (TDMA). This means that each carrier (there is a carrier every 200 KHz) is shared in time by several users, in this case each TDMA frame is divided in 8 intervals. The intervals are known as timeslots, each timeslot constitutes a physical channel. The bit sequence that is transmitted in a timeslot is called burst, this sequence generally is composed of 148 bits plus a guard period corresponding to 8.25 bits.

There are 5 kinds of burst in GSM; however for this work just two of them are important, the Normal Burst and the Access Burst. The Normal Burst is used to transmit traffic and control channels and it is composed of 116 data bits, 3 tail bits at the beginning and end, and 26 bits called "Training sequence bits". The Access Burst is used to access the system and is composed of 36 data bits, 3 tail bits at the beginning and end, and 41 bits called "Synchronization sequence".

Furthermore, the different types of information which are sent over the physical channels are named logical channels. There are many types of logical channels, however in this work only three of them are used, the RACH ("Random Access Channel"), the AGCH ("Access Grant Channel") and the SDCCH ("Stand Alone Dedicated Channel"). The RACH is used to process the unscheduled requests from the mobile station to the network, it is the channel used to send the Access Burst. The AGCH is responsible for allocating resources to the mobile station which previously requested the establishment of communications. The SDCCH is used to exchange data between the mobile station and the network before assigning a traffic channel.

Finally, it is necessary to know that in GSM the information is coded before it is sent. In the case of control channels (which are used in this case) the 184 data bits are converted in 456 coded bits, which are distributed in 4 Normal Burst to be sent. Furthermore, GSM uses GMSK (Gaussian Minimum Shift Keying) modulation; this type of modulation is the same as MSK (Minimum Shift Keying) with a Gaussian filter before the modulation process.

C.4. Resources used

In this work it has been used different tools, both hardware and software. As noted above, our SDR platform consists of the NI USRP-2920 transceivers (it is necessary using 4) and LabVIEW (a graphical development environment). Furthermore, we used the signal analyzer Agilent VSA 89600 [24] for testing the data transmission. Finally, to control LabVIEW and the USRP-2920 it is necessary to use 2 laptops, and the signal analyzer is controlled by the computer placed in the lab.

C.5. Project development

First of all, it is necessary looking for information about the "Location Update" procedure in order to know how to start the development of the work. This procedure involves a message exchange between the Mobile Station and the Network. We can see the messages used in the communication in the Figure 66.

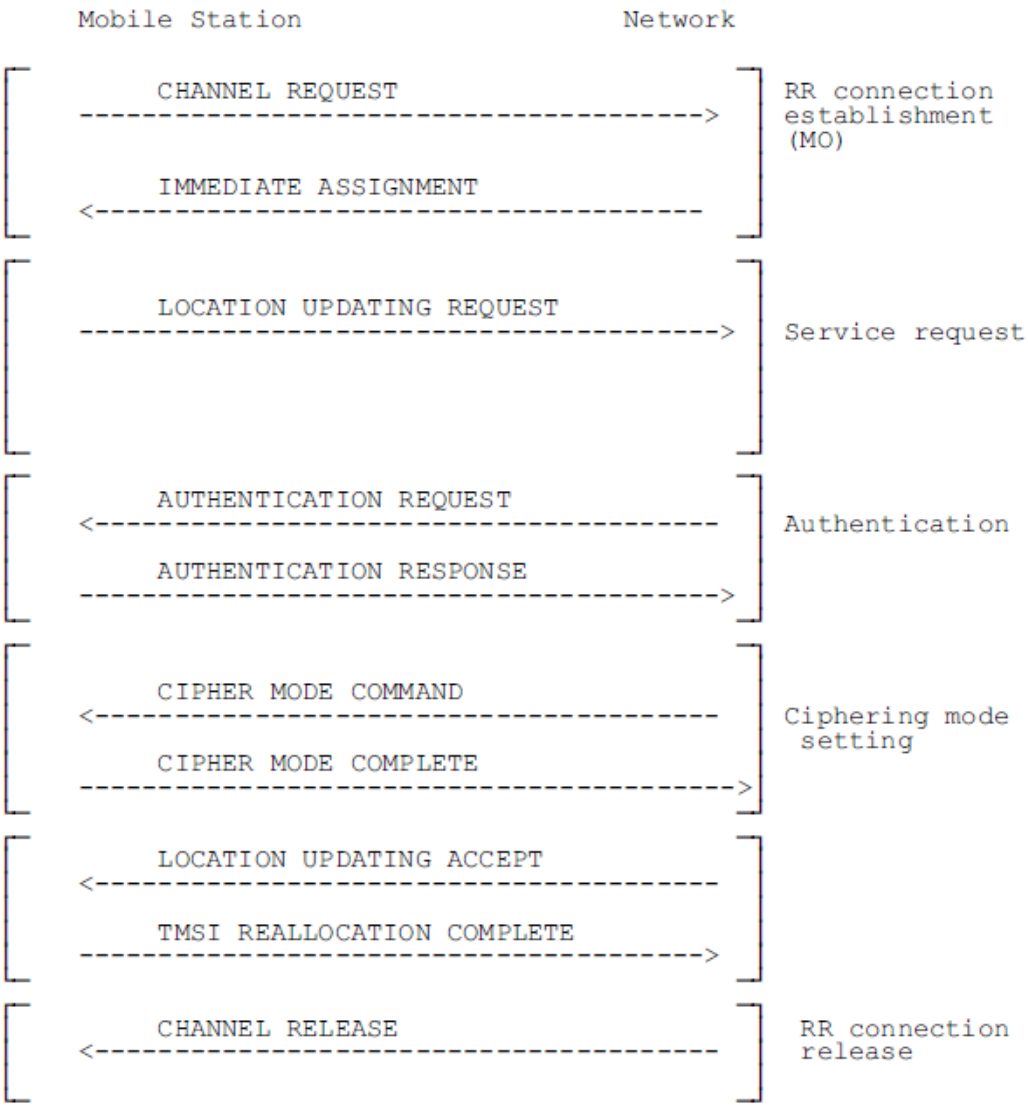

Figure 66: GSM "Location Update" procedure [26]

Once we know the messages that are exchanged in the procedure, it is necessary to know how the massages are formed and which way they follow since they are created until they are sent. We can find this information in all the documents about the GSM standard which are available in ETSI website.

The procedure done in this work can be resumed in the next steps:

1. Create the message by filling it with all the fields listed in the standard according to each case.
2. Encoding the message created using the corresponding algorithms depending on the logical channel used.
3. Burst creation.
4. Burst modulation.
5. Adding the modulated burst into a slot.
6. Join 8 slots to create a frame.
7. Send the frames through the USRP-2920.
8. Receive the frames through the USRP-2920.
9. We obtain the message by comparing the received frame with a fixed pattern present in the message.
10. We decode the message and obtain the original data.

To perform the step 1 it is necessary to consult the document *GSM 04.08 – Mobile Radio Interface* [26], in which the content of each message is explained. After this, we create a LabVIEW block that is responsible for creating all the messages.

In step 2 we follow the steps outlined in the document *GSM 05.03 – Channel coding* [35]. In this case we create three LabVIEW blocks, one for the RACH encoding, one other for the AGCH encoding, and one other for the SDCCH encoding.

To perform the step 3 we create another LabVIEW block with the help of the document *GSM 05.02 - Multiplexing and multiple access on the radio path* [34], which indicates the burst type we need to create (Normal Burst or Access Burst) and how it must be created.

In step 4 we use a GMSK modulator implemented with the modulating tools that LabVIEW provides. This modulator receives a burst and returns the waveform corresponding to it.

To complete the step 5 and create the slot, we just add the guard period once the bursts are modulated.

In the step 6 we concatenate the created slots in the previous step to create a GSM frame (8 slots).

In the steps 7 and 8 we use the tools incorporated in LabVIEW to control the USRP-2920 transceivers. Therefore, we just need to set some parameters to configure the transmission and reception.

To complete the step 9 we compare the received data with a fixed pattern present in the message to know what frame is been sent in this moment.

Finally, in the step 10 we use other LabVIEW blocks to reverse the encoding and the burst creation. This way we can get the original message.

Once all steps are implemented we only have to create the final program in which all the process is done. This program is divided into two parts, the MS and the BTS. Each one must be run simultaneously on two different computers. Thus, thanks to the USRP-2920 transceivers, we can perform a communication between both sides.

The steps followed in each part are the same as described above, but in this case must be performed once for each message. To achieve this, it is expected to receive a message to start sending the next. When the last message is received we consider that the procedure is over.

We can see the "MS.vi" and "BTS.vi" user interface in Figures 67 and 68.

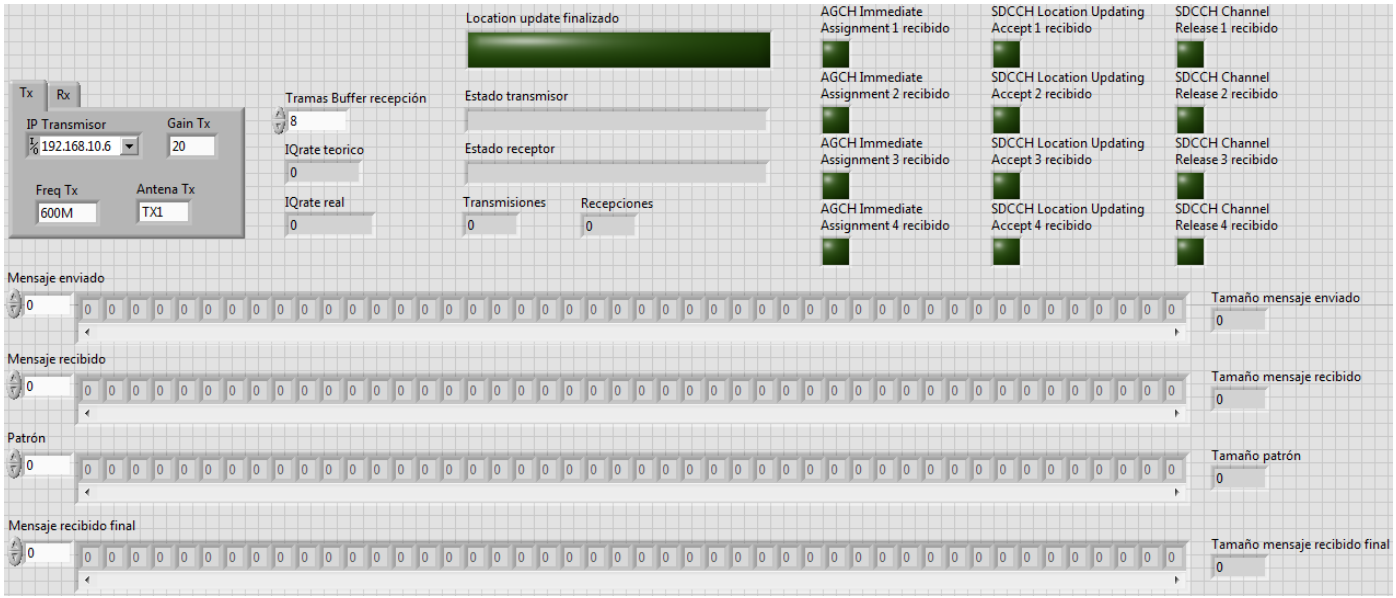

Figure 67: "MS.vi" (Front Panel)

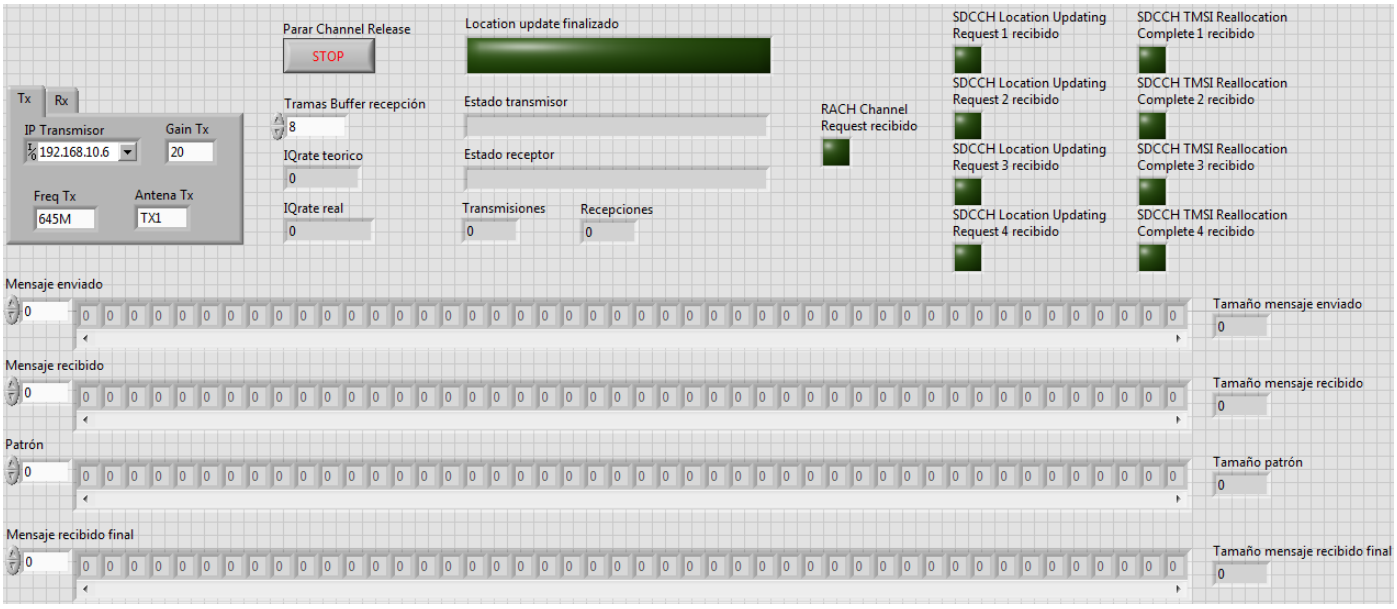

Figure 68: "BTS.vi" (Front Panel)

C.6. Checks and test

During the fulfillment of the TFG, all block that form the program have been tested after they were completed. Thus, it was intended to develop the program with a good base, avoiding mistakes in previous steps once it was advanced.

Early tests focus on coding block. What we do is checking the size of the array of bits in each part of the coding block to see if it has the expected size according to the specifications. One of the most important parts is the interleaving in the AGCCH and SDCCH blocks, in this case the test consist on checking the output of this step in every case and see if it is the same as we can see in the Table 1 of the document *GSM 05.03- Channel coding*.

We test modulation and demodulation by creating a specific block in which we put together the modulation and demodulation blocks. This way, we can insert an array into the modulation block and the output is inserted into demodulation block. If the output of demodulation block is the same as the input of modulation block, the process works properly.

Tests on the final program are the most important because the success of the work depends on them. Although the latter program is a test in itself, since it uses all the implemented blocks, some additional tests are done to see if we get what we expect. First, although it is a bit basic, we test that communication takes place at the desired frequencies, which are 600 MHz for the uplink (MS -> BTS) and 645 MHz for the downlink (BTS -> MS). To verify it, we use the Agilent VSA 89600 signal analyzer and, as we expected, the results are positive. Another test made with the signal analyzer is see graphically how different are the Access Burst and the Normal Burst. As seen, the Access Burst contained less information than the others, since his guard period is much bigger. With the signal analyzer it could also be observed that the theory is fulfilled in practice and the Access Burst is smaller than the Normal Burst.

After seen that radio transmission and reception work properly, we passed to run the main program to see if it works as expected. For testing, we run both VI ("MS.vi" and "BTS.vi") at a time, so that the MS starts sending the "Channel Request" and waiting the "Immediate Assigment" and the BTS awaits the "Channel Request" to send the "Immediate Assigment". The program works as expected and the indicators are progressively turning on while the procedure advances till it finishes, moment in which all the LEDs are lit. Therefore, we can conclude that the program meets expectations.

C.7. Conclusions

In last section we have seen how the program worked correctly and the process is completed. For this, we created two different user interfaces which were run in two different computers. Furthermore, the user interface allows the user to modify some of the main communication settings. However, some of the parameters that cannot be manipulated in the user interface (such as the message elements) can be easily changed with minor modifications of the code by anybody without previous knowledge about LabVIEW.

As for the tools used in the project, it was easy to use them without any previous knowledge about them. In addition, the completion of this project has helped the student to get new and interesting knowledge about the SDR technology and the GSM workings.

Furthermore, this paper leaves open a large number of possible future work lines such as the development of new procedures which use other logical channels, or adding a second BTS to this work and see how the “Location Update” procedure takes place in reality.

Referencias

[1] I. Morcillo Gutierro, «TFG - Implementación de un receptor simple GSM mediante plataforma Software Defined Radio - Grado en Ingeniería en Tecnologías de Telecomunicación,» Leganés, 2014.

[2] ETSI, «Mobile technologies GSM,» [En línea]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile/gsm. [Último acceso: 7 8 2015].

[3] ETSI, «UMTS,» [En línea]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile/umts. [Último acceso: 7 8 2015].

[4] J. Wannstrom, «HSPA,» [En línea]. Available: http://www.3gpp.org/technologies/keywords-acronyms/99-hspa. [Último acceso: 7 8 2015].

[5] ETSI, «Long Term Evolution,» [En línea]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile/long-term-evolution. [Último acceso: 7 8 2015].

[6] M. Dillinger, K. Madani y N. Alonistioti, Software Defined Radio: Architectures, Systems and Functions, WILEY, 2003.

[7] National Instruments, «Software de Desarrollo de Sistemas NI LabVIEW,» [En línea]. Available: http://www.ni.com/labview/esa/. [Último acceso: 12 8 2015].

[8] National Instruments, «USRP-2920,» [En línea]. Available: http://sine.ni.com/nips/cds/view/p/lang/es/nid/212995. [Último acceso: 12 8 2015].

[9] GNU Radio, «GNU Radio,» [En línea]. Available: http://gnuradio.org/redmine/projects/gnuradio. [Último acceso: 3 4 2015].

[10] GNU, «GNU Octave,» [En línea]. Available: https://www.gnu.org/software/octave/. [Último acceso: 3 4 2015].

[11] MathWorks, «Matlab,» [En línea]. Available: http://es.mathworks.com/products/matlab/. [Último acceso: 7 8 2015].

[12] SDR-RADIO.com, «SDR-RADIO.com,» [En línea]. Available: http://sdr-radio.com/. [Último acceso: 12 8 2015].

[13] Grupo de Políticas Públicas y Regulación, «La gestión de derechos de propiedad intelectual en el entorno TIC,» Madrid, 2014.

[14] BOE, «Ley General de Telecomunicaciones,» 5 2014. [En línea]. Available: https://www.boe.es/boe/dias/2014/05/10/pdfs/BOE-A-2014-4950.pdf. [Último acceso: 7 8 2015].

[15] BOE, «Real Decreto 1066/2001,» 9 2001. [En línea]. Available: https://www.boe.es/boe/dias/2001/09/29/pdfs/A36217-36227.pdf. [Último acceso: 7 8 2015].

[16] National Instruments, «NI USRP-292x/293x Datasheet,» [En línea]. Available: http://www.ni.com/datasheet/pdf/en/ds-355. [Último acceso: 22 8 2015].

[17] Ingeniería de Sitemas, «Tecnología GSM,» [En línea]. Available: http://eve-ingsistemas-u.blogspot.com.es/2012/04/el-sistema-global-para.html. [Último acceso: 7 8 2015].

[18] Departamento de Teoría de la Señal y Comunicaciones, «Tema 4 - Redes de comunicaciones móviles terrestres,» Leganés, 2014.

[19] Departamento de Teoría de la Señal y Comunicaciones, «Tema 3 - GSM (parte 1) - Arquitectura y servicios,» Madrid, 2015.

[20] Tutorials Point, «GSM - The Mobile Station,» [En línea]. Available: http://www.tutorialspoint.com/gsm/gsm_mobile_station.htm. [Último acceso: 10 8 2015].

[21] MSTAR::UNEX, «Multiobjective Frequency Assignment Problem,» [En línea]. Available: http://mstar.unex.es/index.php?option=com_content&view=article&id=59&Itemid=55. [Último acceso: 7 8 2015].

[22] Departamento de Teoría de la Señal y Comunicaciones, «Tema 3 - GSM (parte 2) - Interfaz radio,» Leganés, 2015.

[23] National Instruments, «Device Specifications. USRP-2920,» [En línea]. Available: http://www.ni.com/pdf/manuals/375839a.pdf. [Último acceso: 6 4 2015].

[24] KeySigth Technologies, «89600 VSA and WLA Software,» [En línea]. Available: http://www.keysight.com/en/pc-1905089/89600-VSA-and-WLA-Software?cc=ES&lc=eng. [Último acceso: 15 8 2015].

[25] Agilent Technologies, «Agilent 89600S Series VXI-Based. Configuration guide,» [En línea]. Available: http://literature.cdn.keysight.com/litweb/pdf/5968-9350E.pdf. [Último acceso: 15 8 2015].

[26] ETSI, «Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification (GSM 04.08),» Julio 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/04/0408/05.03.00_60/gsmts_0408v050300p.pdf.

[Último acceso: 12 5 2015].

[27] ETSI, «Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (GSM 03.03),» Marzo 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0303/05.00.00_60/gsmts_0303v050000p.pdf. [Último acceso: 12 5 2015].

[28] ETSI, «Digital cellular telecommunications system; Restoration procedures (GSM 03.07),» Noviembre 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0307/05.00.00_60/gsmts_0307v050000p.pdf. [Último acceso: 12 5 2015].

[29] ETSI, «Digital cellular telecommunications system (Phase 2+); Organization of subscriber data (GSM 03.08 version 5.1.0),» Abril 1997. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0308/05.01.00_60/gsmts_0308v050100p.pdf. [Último acceso: 12 5 2015].

[30] ETSI, «Digital cellular telecommunications system; Location registration procedures (GSM 03.12),» Noviembre 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0312/05.00.00_60/gsmts_0312v050000p.pdf. [Último acceso: 12 5 2015].

[31] ETSI, «Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 8.1.0 Release 1999),» Julio 2001. [En línea]. Available: http://www.etsi.org/deliver/etsi_ts/100900_100999/100929/08.01.00_60/ts_100929v080100p.pdf. [Último acceso: 12 5 2015].

[32] ETSI, «Digital cellular telecommunications system; Functions related to Mobile Station (MS) in idle mode and group receive mode (GSM 03.22 version 5.0.1),» Mayo 1997. [En línea]. Available: http://www.etsi.org/deliver/etsi_i_ets/300900_300999/300930/01_60/ets_300930e01p.pdf. [Último acceso: 12 5 2015].

[33] ETSI, «Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description (GSM 05.01 version 5.4.0),» Abril 1998. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/05/0501/05.04.00_60/gsmts_0501v050400p.pdf. [Último acceso: 12 5 2015].

[34] ETSI, «Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path (GSM 05.02),» Agosto 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/05/0502/05.01.00_60/gsmts_0502v050100p.pdf. [Último acceso: 12 5 2015].

[35] ETSI, «Digital cellular telecommunications system (Phase 2+); Channel coding (GSM 05.03),» Agosto 1996. [En línea]. Available:

http://www.etsi.org/deliver/etsi_gts/05/0503/05.02.00_60/gsmts_0503v050200p.pdf. [Último acceso: 12 5 2015].

[36] ETSI, «Digital cellular telecommunications system (Phase 2+); Modulation (GSM 05.04 version 8.1.2 Release 1999),» Febrero 2001. [En línea]. Available: http://www.etsi.org/deliver/etsi_en/300900_300999/300959/08.01.02_60/en_300959v080102p.pdf. [Último acceso: 12 5 2015].

[37] ETSI, «Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification (GSM 09.02),» Agosto 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/09/0902/05.03.00_60/gsmts_0902v050300p.pdf. [Último acceso: 12 5 2015].

[38] National Instruments, «Aprenda LabVIEW,» [En línea]. Available: http://www.ni.com/academic/students/learn-labview/esa/. [Último acceso: 2 4 2015].

[39] ITU, «Indicativos de red para el servicio móvil (MNC) del plan de identificación internacional para redes públicas y usuarios (Según la Recomendación UIT-TE.212 (05/2008)),» 2001. [En línea]. Available: http://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.212B-2011-PDF-S.pdf. [Último acceso: 16 8 2015].